POD Maatschappelijke Integratie
SPP Intégration Sociale

Aan de dames en heren voorzitters van de openbare centra voor maatschappelijk welzijn en de DPO's

Hebt u vragen? Nood aan bijkomende info?
Stuur een mail naar de DPD op het volgende adres
MI.DPO@mi-is.be
Of bel naar 02 508 84 30

Datum: 07/12/2022

Aanwijzingen voor het opslaan van gegevens

om het hoofd te bieden aan een ernstige gebeurtenis waarbij werkgegevens verloren gaan of niet toegankelijk zijn.

Mevrouw de Voorzitster,
Mijnheer de Voorzitter,

Cyberaanvallen bedreigen alle sectoren en de OCMW's ontsnappen hier helaas niet aan. Recente gebeurtenissen herinneren ons eraan dat de gevolgen van deze aanvallen desastreus kunnen zijn voor uw administratie en bijgevolg voor de rechthebbenden.

De POD Maatschappelijke Integratie informeert u over goede praktijken om u te beschermen tegen de verwoestende gevolgen van dergelijke aanvallen:

- Ten eerste door u eraan te herinneren hoe u zich moet voorbereiden op elke aanval, en welke acties u moet ondernemen in geval van een aanval;
- Ten tweede door u eraan te herinneren hoe u uw gegevens moet beschermen om de beschikbaarheid en integriteit ervan te waarborgen, d.w.z. door correct uitgevoerde back-ups.

1. EEN CYBERAANVAL HET HOOFD BIEDEN

Ongeacht de grootte van uw OCMW is het belangrijk om voorbereid te zijn op een cyberaanval en de juiste preventieve maatregelen te nemen.

1.1. NUTTIGE DOCUMENTEN

Om u te helpen zijn er verschillende aanbevelingen van de Belgische overheidsinstanties die belast zijn met cyberveiligheid. Wij verzoeken u om de informatie op deze pagina's te raadplegen:

- https://cyberguide.ccb.belgium.be/nl en https://cyberguide.ccb.belgium.be/nl/plan-uw-beveiliging-0
- https://www.cert.be/nl/richtlijnen

POD Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid
Administratief Centrum Kruidtuin - Finance Tower
Kruidtuinlaan 50 bus 165
B - 1000 Brussel | T. +32 2 508 85 85 | vraag@mi-is.be | www.mi-is.be

- In zeer problematische gevallen van ransomware: https://www.cert.be/nl/paper/ransomware-bescherming-en-preventie

Naast de praktische maatregelen die in deze documenten worden beschreven, wordt aanbevolen dat u:

- Over een procedure beschikt voor het beheer van inbreuken op de beveiliging ("security breach management policy"), om het incident zo snel mogelijk te identificeren en de juiste mensen op de hoogte te brengen.
- Over een bedrijfscontinuïteitsplan ("Business Continuity Plan" of "BCP") beschikt, om de kernactiviteiten te beschermen in een incidentensituatie, althans in verminderde modus. Het doel hiervan is de schade te beperken en de onderneming in staat te stellen de "normale" activiteiten zo snel mogelijk te hervatten.
- Over een disaster recovery plan (DRP) beschikt, zodat het bedrijf snel en volledig opnieuw kan opstarten.

Gezien het belang van ransomware-aanvallen en de rampzalige gevolgen ervan, raden wij u aan het document te downloaden en te raadplegen dat beschikbaar is op
https://www.cert.be/sites/default/files/ransomware_2019_nl.pdf.
Het bevat waardevolle adviezen en verschillende soorten informatie om u te helpen uw verdediging tegen deze bijzonder brutale en rampzalige aanvallen te organiseren. .
Daarnaast heeft het CCB (Centre for Cybersecurity Belgium) een bijzonder praktisch document gepubliceerd met een actieplan van 12 punten dat onmiddellijk moet worden uitgevoerd in geval van een aanval (https://cert.be/sites/default/files/steps_to_take_in_case_of_ransomware_attack_def_nl.pdf).

1.2. WIE VERWITTIGEN BIJ EEN AANVAL?

Ter herinnering: er bestaat ook een verplichting om het incident te melden aan een toezichthoudende autoriteit en/of aan personen die mogelijk worden getroffen door de gevolgen van het incident (bv. op grond van, op basis van de AVG en/of de NIS-richtlijn - en de Belgische omzettingswetgeving daarvan).
In geval van een veiligheidsincident moet u zich de vraag stellen of uw onderneming wettelijk verplicht is tot kennisgeving of niet.

4 STAPPEN:
1° Het incident identificeren en de interne procedure voor de behandeling van incidenten opstarten
2° de wettelijke verplichtingen van uw OCMW identificeren en naleven
3° Klacht indienen / het incident melden (https://www.cert.be/nl/een-incident-melden)
4° Zorgen voor een goede crisiscommunicatie en jouw reputatie behouden

Onmiddellijke reactie: zie https://www.cert.be/nl/eerste-hulp-bij-een-cyberaanval

Plan voor back-ups: zie CCB: https://cyberguide.ccb.belgium.be/nl/maak-back-alle-0

ALTERNATIEF VOOR EEN ANTWOORDPLAN:
https://cert.be/sites/default/files/steps_to_take_in_case_of_ransomware_attack_def_nl.pdf

2. BEHEER VAN HET OPSLAAN VAN GEGEVENS

Een goede gegevensopslag met een beproefd plan voor de uitvoering ervan is essentieel om de gevolgen van het stilleggen van het systeem en het niet beschikbaar zijn van informatie, wat een onderbreking (of ten minste een verstoring) van de dienstverlening inhoudt, te voorkomen of althans tot een minimum te beperken:

- Bij verlies van gegevens door een (meestal menselijke) fout
- In het geval van een verwerkingsfout met betrekking tot een grote hoeveelheid gegevens
- In het geval van schade als gevolg van een cyberaanval, met name de schade die wordt veroorzaakt door ransomware.

Naast de garanties die een dergelijk back-upplan biedt op het gebied van beschikbaarheid en integriteit van de gegevens, zal het u in staat stellen uw activiteiten voort te zetten zonder uw gebruikers te schaden en zonder de reputatie van uw diensten te schaden.

Het plan voor de back-up van gegevens zal worden opgenomen in de plannen Business Continuity Plan en Disaster Recovery Plan (zie hieronder).

1.1. PRINCIPES

De definitie van een back-upschema moet gebaseerd zijn op een overeenkomst met de gehele organisatie over de aanvaarde duur van de gegevens die verloren mogen gaan (RPO) en de tijd voor het hervatten van de normale werkzaamheden (WRT).

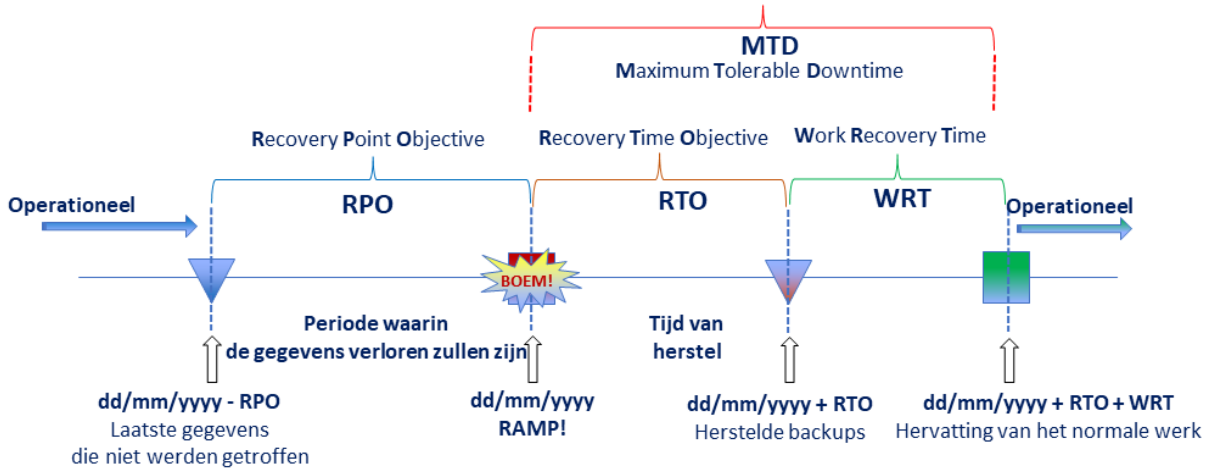
Deze overeenkomst kan worden geformaliseerd in een Service Level Agreement (SLA) wanneer de back-up wordt beheerd door een externe dienstverlener.

De volgende termen worden over het algemeen gebruikt om de parameters van de uit te voeren back-ups te definiëren:

RPO: Recovery Point Objective:
De maximale periode waarin het OCMW accepteert dat gegevens verloren mogen gaan
RTO: Recovery Time Objective:
De maximaal toegestane tijd om vanuit een back-up te herstellen
WRT: Work Recovery Time:
De tijd die na het herstel van de gegevens nodig is om alles te reconstrueren en een volledige en operationele organisatiecontext te herstellen

Deze parameters worden nader uitgewerkt in een formeel document dat wordt gesloten met de (interne of externe) entiteit die verantwoordelijk is voor deze back-ups en waarin de volgende afspraken worden vermeld
SLA: Service Level Agreement:
contract tussen OCMW en leverancier waarin alle afspraken, zoals SLO's, wachtdiensten, kosten, enz. worden vastgelegd
SLO: Service Level Objective:
beschrijft in de SLA meetbare technische doelstellingen zoals RPO, RTO, bandbreedte.

Het volgende schema brengt deze verschillende parameters in verband met een tijdlijn.



1.2. VAN WELKE GEGEVENS EEN BACKUP MAKEN?

Het OCMW verwerkt gegevens door middel van systemen die door eigen personeel of door een IT-onderaannemer worden beheerd.

Deze omvatten:

- de softwareproducenten
- de IT-diensten van de stad of gemeente waartoe het OCMW behoort.
- een dienst in de Cloud.

In deze gevallen worden de back-ups verzorgd door deze onderaannemers in het kader van de tussen het OCMW en de verantwoordelijke voor de verwerking, het OCMW, vastgestelde SLA.

Met deze informatie kan de DPO van het OCMW ervoor zorgen dat hij voldoende garanties heeft van zowel zijn onderaannemers als de persoon of personen die verantwoordelijk zijn voor de lokale gegevensback-up.

BELANGRIJKE OPMERKING: De volgende informatie is vooral bedoeld voor het OCMW, dat zelf de nodige back-ups moet maken om de gevolgen van een cyberaanval te beperken of zelfs te elimineren.

Soorten gegevens

De gegevens die moeten worden opgeslagen zullen afhankelijk van hun aard verschillend worden behandeld, idealiter volgens een classificatie die voldoet aan de minimale KSZ-normen (https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/bld_data_data_classificatie.pdf)

We onderscheiden minstens de 3 volgende soorten gegevens:

- “Systeem”-gegevens;
- Niet-gevoelige maar belangrijke gegevens van het OCMW;
- Persoonlijke gegevens. Deze laatste vereisen speciale voorzorgsmaatregelen en bepalingen om te voldoen aan de vereisten van de GDPR.

1.3. STRATEGIE EN SOORTEN BACKUPS

De strategie “1-2-3”

De aanbevolen strategie komt overeen met het volgende schema:

Een externe back-up is essentieel om besmetting van de back-upbestanden in geval van bijvoorbeeld ransomware te voorkomen.

Er zijn verschillende soorten back-ups:

Soorten back-ups

De volledige back-up

Een volledige back-up slaat telkens een volledige kopie op van de databanken, bestanden en informatie van het computersysteem, volgens een geprogrammeerde periodiciteit. Hoewel de back-uptijd langzamer is en de back-up meer opslagruimte vereist, is het voordeel van de volledige back-up dat de herstelopera ties sneller en eenvoudiger zijn.

De incrementele back-up

De oorspronkelijke back-up is voltooid en vervolgens worden bij elke volgende back-up alleen de wijzigingen opgeslagen die sinds de laatste back-up werden aangebracht.

De back-up is sneller omdat er minder gegevens moeten worden opgeslagen. Het is daarom ook de methode die de minste opslagruimte vereist, maar het duurt langer om de gegevens te herstellen.

De differentiële back-up

Net zoals de incrementele methode is de eerste back-up volledig. Maar daarna maakt het systeem een back-up van alle wijzigingen sinds de laatste volledige back-up. Dit type back-up vereist meer opslagruimte dan de incrementele, maar maakt het mogelijk om de gegevens sneller te herstellen.

Rotatie van de back-updragers

Back-ups worden gemaakt volgens een rotatieschema van de dragers dat het model, de frequentie en het rotatiepatroon specificeert, zoals:

First in, first out (FIFO)

Nieuwe of gewijzigde bestanden worden opgeslagen op de drager dat de oudste - en dus minst bruikbare - opgeslagen gegevens bevat. Dit is het eenvoudigste rotatieschema.

> ***Voorbeeld: elke back-up wordt op een andere drager uitgevoerd;*** *een dagelijkse back-up op een totaal van 14 mediadragers biedt een back-up van 14 dagen.*
>
> *Elke dag wordt de drager met de oudste informatie ingevoegd wanneer de back-up wordt uitgevoerd.*

Grootvader - vader - zoon

Er zijn minstens drie back-upcycli: dagelijks, wekelijks en maandelijks. Dagelijkse back-ups maken gebruik van wisselende media zoals hierboven beschreven).

Wekelijkse back-ups worden ook wekelijks afgewisseld.

Maandelijkse back-ups worden maandelijks afgewisseld.

Afzonderlijke back-ups kunnen ook voor langere periodes worden gepland: driemaandelijks, halfjaarlijks en/of jaarlijks.

Dit is het meest gebruikelijke rotatieschema voor back-updragers.

Er bestaan ook nog andere methodes (cf. De Toren van Hanoi): zij hebben steeds tot doel de back-upcyclus te optimaliseren.

1.4. BACK-UPPLAN EN -PROCEDURE

Zoals in alle aanbevelingen staat, moet de aanpak voor het maken van back-ups worden gedocumenteerd. Deze documentatie bestaat uit een back-upplan dat door de directie is goedgekeurd en gevalideerd, en een beschrijving van de procedure(s) waarin alle parameters en handelingen die voor het maken van back-ups moeten worden uitgevoerd, gedetailleerd worden beschreven.

Deze documentatie zal een gemakkelijke en ondubbelzinnige overdracht mogelijk maken in geval van overdracht van verantwoordelijkheid, bij afwezigheid, vertrek, enz.)

Het back-upplan zal het volgende vermelden:

- De lijst van gegevens (en hun type) waarmee rekening wordt gehouden voor de back-up;
- het back-upmodel (“Volledig”, “Incrementeel”, “Differentieel”) en hun rotatieschema (zie volgende dia);
- de procedure waarin de deelnemers, hun respectieve acties en verantwoordelijkheden en de regelmatig uit te voeren controles worden gespecificeerd;
- de opslagfaciliteiten en het beheer daarvan (toegang, behandeling, locatie, enz.);
- de procedures voor herstelonderzoek met geldigheidstesten;
- de vernietiging van alle dragers die gegevens hebben bevat.

De logboeken, die samen met de back-upmedia worden bewaard, bevatten ten minste de volgende informatie:

- referenties van de back-upvoorziening
- betrokken perimeter of onderdelen
- soort back-up;
- geback-upte bestanden;
- datum van de back-up;
- status van de back-up.

1.5. "IN-SITU" BACK-UP VAN LOKALE GEGEVENS

Wanneer het OCMW gegevens verwerkt die essentieel zijn voor de continuïteit van zijn activiteiten zonder dat door IT-dienstverleners een back-up wordt verstrekt, moeten de back-upplannen, -procedures en -middelen die lokaal worden gebruikt, worden vastgesteld en uitgevoerd.

PC opslaan op externe harde schijf

In de praktijk biedt de huidige technologie van via USB 3.0 aangesloten externe harde schijven snelle en eenvoudige back-upmogelijkheden tegen relatief lage kosten, terwijl de hierboven beschreven aanbevelingen, soorten en rotaties worden ondersteund.

Softwareoplossing voor back-up:

Er zijn een aantal oplossingen, zowel betaalde als FOSS (Free Open-Source Software), afhankelijk van de verwachte ondersteuningsbehoeften.

Aanbevolen soort back-up

Het soort back-up dat het meest lijkt te worden aanbevolen om te voorkomen dat te grote volumes worden overgebracht en toch voldoende granulariteit te bieden, is een "volledig + incrementeel" back-upschema.

Over het algemeen wordt een "volledig plus differentieel" schema geschikter geacht voor grotere organisaties die over meer IT-middelen beschikken.

Aanbevolen rotatieschema

Het voorgestelde rotatieschema is "**Grootvader - vader - zoon**". Ook al zijn de herstelmogelijkheden trager, het vereiste opslagvolume is veel kleiner en dus is de mogelijkheid om oudere kopieën te bewaren veel groter, wat in sommige gevallen een gelegenheid kan zijn.

In ieder geval moeten maatregelen worden genomen om ervoor te zorgen dat een dataset buiten het OCMW wordt opgeslagen, bijvoorbeeld in een kluis van de gemeente/stad waartoe het OCMW behoort.

... en natuurlijk, documenteren met plannen en procedures, alle betrokkenen opleiden en regelmatig hersteltesten uitvoeren om ervoor te zorgen dat alles onder controle is en werkt zoals verwacht.

Moeten gegevens worden versleuteld wanneer een back-up wordt gemaakt?

Gegevens die als "vertrouwelijk" zijn aangeduid, worden vooraf versleuteld, zodat het bij eventuele diefstal van de schijf onmogelijk is deze gegevens terug te halen. De eenvoudigste oplossing, zonder extra kosten, is om "Bitlocker" van Microsoft te gebruiken om de schijven te vergrendelen.

Cloud of geen Cloud?

Een back-up in de Cloud, die waarschijnlijk duurder is, zal ook vereisen dat gegevens die als "vertrouwelijk" worden geclassificeerd vooraf worden versleuteld.

Hebt u nog vragen over cyberaanvallen of over het nemen van een back-up van uw gegevens?
Neem dan contact op met de POD Maatschappelijke Integratie, Armoedebestrijding en Grootstedenbeleid

- Per mail: MI.dpo@mi-is.be
- Telefonisch: + 32 2 508 85 85 van 8.30 uur tot 12.30 uur en van 13 uur tot 16.30 uur (op vrijdag tot 16 uur)

Hoogachtend,

Getekend

Alexandre LESIW
Voorzitter