BUSSINESS CONTINUITY DOSSIER

Youth energy

NHL-Stenden * Rengerslaan 10 * 8917DD Leeuwarden

[Website-hyperlink]

Wiljan Siderius, Leon Dijkstra, Lukas Cremers, Stefan Suk, Bram Bram

Versie 1 (05-04-2024)

Inhoud

1. Instructies gebruik plan

In dit hoofdstuk worden de basisstappen voor gebruik van dit plan benoemt en hoe er dient te worden gehandelt.

1.1 Het in werking stellen van het plan

Dit plan wordt geïnitieerd bij rampscenario's en blijft van kracht totdat werkzaamheden op normale manier hervat kunnen worden.

1.2 Kennisgeving tijdens incident

Verantwoordelijkheden van aanwezig personeel tijdens/buiten kantooruren:

Na observatie van een mogelijk kritische situatie, wordt het crisisteam ingelicht.

Valt het incident/de ramp zich plaats buiten kantooruren, wordt contact opgenomen met het crisisteam.

De volgende informatie zal worden verschaft aan het crisisteam:

- Locatie van de ramp
- Soort ramp
- Vat de schade samen (bijvoorbeeld matig/zwaar)

Vervolgens wordt de calamiteit opgenomen door het crisisteam en wordt het Disaster recoveryplan in werking gezet.

1.3 Verantwoordelijkheden teamleden

- Elk teamlid houdt een bijgewerkte lijst met telefoonnummers bij van zijn/haar afdeling. Dit geld voor zowel mobiel als thuis.

- Elk teamlid houdt een fysiek exemplaar bij zich thuis voor het geval dat er een incident zich voor doet buiten werktijd. Alle teamleden zullen zich bekend moeten maken met de inhoud van het plan.

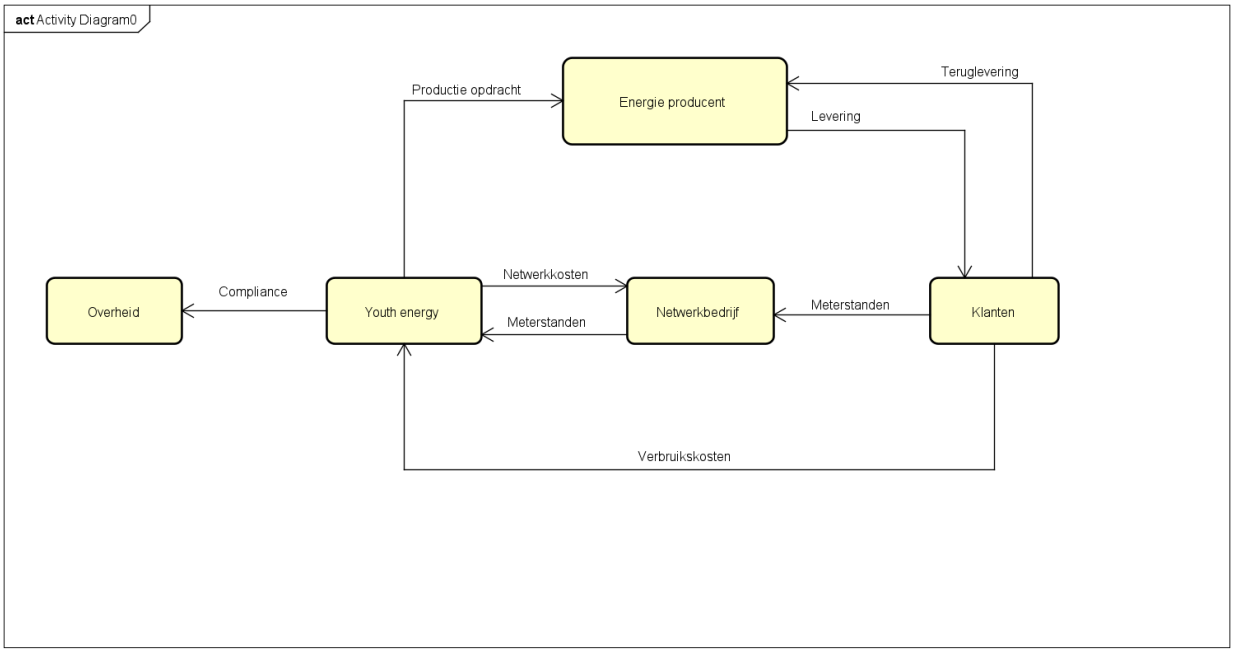
2. Business continuity management voor Youth energy

2.1 Cruciale processen

Youth energy heeft als opdracht het leveren van energie en het geven van advies aan potentiële klanten.

De hoofdzaken waar Youth energy zich mee bezig houdt zijn:

- Het leveren van energie aan klanten: Youth energie is een energieleverancier die haar klanten voorziet van elektriciteit en gas.
  Youth energy voert dit proces uit in samenwerking met een energieproducent.
  Input: Productieopdracht
  Output: Verbruikskosten



- Het uitlezen van slimme meter: Om het verbruik van klanten in kaart te kunnen brengen en klanten de juiste afschrijving te kunnen schrijven moet Youth energie de slimme meter van haar klanten uitlezen. Dit gebeurt in vaste intervallen.
  Dit proces wordt uitgevoerd in samenwerking met de netwerkbeheerder.
  Input: Uitlees verzoek
  Output: Meterstand die wordt geupdate/toegevoegd aan de klant data.

- Klanten inzicht geven in hun energie gebruik: Youth energie wil haar klanten inzicht geven in hun verbruik, de mate van precisie van tijd ligt aan het uitlees interval van de slimme meters.
- Service verlenen aan klanten: Wanneer klanten van youth energy vragen hebben of complicaties moeten deze klanten geholpen kunnen worden. Als deze klanten niet binnen een redelijke tijd geholpen kunnen worden kan dat leiden to onvrede en potentieel klantverlies.
  Input: Klantenservice medewerkers die paraat staan voor klanten.
  Output: Klanten die geholpen worden bij een vraag/probleem.

Deze hoofdzaken zijn cruciaal voor het staande houden van het bedrijf en moeten binnen 24 uur worden hersteld bij calamiteiten

2.2 Sub-proces

Naast deze cruciale taken geeft Youth energy ook processen die niet cruciaal zijn voor het blijven staan van het bedrijf maar die wel belangrijk zijn voor haar identiteit tegenover de klanten.

Deze processen zijn:

- Het geven van advies aan klanten: Youth energie is een energieleverancier die het als haar verantwoordelijkheid ziet om de wereld een stukje groener te maken. Dit wil ze bereiken door haar klanten helpen met het verduurzamen van hun huis door middel van het geven van adviezen.
  Input: Verduurzaming experts die paraat staan voor klanten om te adviseren.
  Output: Klanten die na het advies weten hoe ze kunnen verduurzamen.

- Het uitbreiden van klantenaantal: Youth energie wil blijven groeien en investeert daarom in het marketen om nieuwe klanten te krijgen.
  Input: Geografisch onderzoek met als gevolg investering in marketen in doelgebieden.
  Output: Meer klant aanmeldingen

2.3 Proceseigenaar

Binnen youth energy was Martin molema de eigenaar van alle processen echter door een transitie in management is dit recentelijk overgedragen aan Sander ten Hoor die de nieuwe proces eigenaar zal is geworden en verantwoordelijkheid draagt voor alle processen.

2.4 Bedrijf afdelingen

Het bedrijf bestaat uit meerdere afdelingen die betrokken zijn bij de bedrijfs processen.

2.4.1 ICT

Deze afdeling houd zich bezig met de ICT zaken binnen het bedrijf en is belangrijk voor de stroming van informatie naar de verschillende afdelingen. Deze afdeling is van hoog belang.

2.4.2 Backoffice

Nog onduidelijk.

2.4.3 Marketing

Deze afdeling is belangrijk voor het promoten van het bedrijf zodat het kan groeien. Deze afdeling heeft beschikking tot publiekelijke geografische data en interne verkoop data.

2.4.4 Verkoop

Deze afdeling is belangrijk voor het verkrijgen van nieuwe klanten.

2.4.5 Human resources

Deze afdeling is belangrijk voor het indelen van werknemers in afdelingen, het behandelen van contractuele evenementen met personeel, etc.

2.4.6 Klantenservice

Deze afdeling is de directe lijn voor klanten die vragen hebben en is dus belangrijk voor het contact met de klant. Deze afdeling is van hoog belang.

2.5 Procesrelaties

Bij de processen zijn bepaalde afdelingen van het bedrijf betrokken en die relaties zullen hier worden duidelijk gemaakt. Afdelingen binnen Youth Energy zullen worden aangegeven met (-) en partijen van buitenaf zullen worden aangegeven met (+).

Het leveren van energy aan klanten
- ICT
-Verkoop
+Energieproducent
+Netwerkbeheerder

Het uitlezen van slimme meter
-ICT
+Netwerkbeheerder

Klanten inzicht geven in hun energie gebruik
-ICT
-Klantenservice
+Netwerkbeheerder

Het geven van adviezen aan klanten
-Klantenservice
-Verkoop

Het uitbreiden van klanten aantal
-Verkoop
-Marketing

2.6 Kritische informatievoorziening

Youth energy is afhankelijk van meerdere bronnen van data en het is daarom van cruciaal belang dat deze data veilig en altijd beschikbaar is.

Back-up gegevens
Het is van uiterst kritiek belang dat de gegevens op minstens 2 verschillende locaties worden opgeslagen ver genoeg uit elkaar dat bij verlies van de één, de ander gelijk bruikbaar is voor de continuïteit van het bedrijf. Deze back-up maatregelingen dienen regelmatig getest te worden.

Meterstand gegevens:
Dit is de belangrijkste bron van informatie voor Youth energie, deze informatie moet altijd kloppen en moet up to date zijn.

Klantengegevens:
Om klanten van dienst te kunnen zijn is het belang van deze klantengegevens cruciaal en het moet altijd kloppend zijn.

Geografische gegevens:
deze gegevens zijn in beheer van de staat en is publiekelijk beschikbaar. Deze informatie is van belang voor marketing om in te kunnen schatten waar het bedrijf kan investeren.

3. Maximum disruption time

In dit hoofdstuk zal worden behandeld wat de maximale onderbrekingstijd van processen mogen zijn, deze zijn bepaald doormiddel van een interview met proceseigenaar Martin Molema (Februari), Sander ten Hoor (Maart) en door middel van Business Impact analyses hieronder te zien. Ook wordt beschreven waarom de processen draaiende moeten worden gehouden en wat de impact kan zijn bij stilstand.

Proces van calamiteit	Kans	Impact financieel	Impact Reputatie	Missie	Recovery Time Objective (RTO)	Recovery point objective (RPO)
Energie leveren aan klanten	Klein	Zeer hoog	Zeer hoog	Zeer hoog	2 uur	-
Het uitlezen van meter	Klein	Zeer hoog	Hoog	hoog	24 uur	1 maand
Klanten inzicht geven in energie gebruik	Marginaal	Marginaal	Hoog	Hoog	7 dagen	-
Service verlenen aan klanten	Klein	Klein	Hoog	Hoog	24 uur	-
Advies geven aan klanten	Klein	Klein	Marginaal	Hoog	7 dagen	-
Uitbreiden van klantenaantal	Klein	Marginaal	Klein	Hoog	12 uur	24 uur

Energie leveren aan klant
Dit is het hoofdproces van het bedrijf, als dit proces te lang uit staat heeft dat catastrofale gevolgen op het financiële-, reputatie- en missiegebied. Aangezien er geen data bij dit proces betrokken is Is er geen RPO.

Uitlezen van de meter
Dit proces is belangrijk om bij te houden hoeveel energie de klant verbruikt heeft en hoeveel er daarom in rekening moet worden gebracht. De kans dat de meters niet meer kunnen worden uitgelezen is vrij klein, als er calamiteiten in dit proces zijn is het van belang dat de meter voor de maandelijkse rekening weer is hersteld aangezien de rekening anders niet kan worden berekend. Aangezien de meterstand lezing ook van belang is voor het verbruiksinzicht van de klant op de webapplicatie wordt er naar gestreefd om dit proces binnen een dag te kunnen herstellen.

Klanten inzicht geven in energie verbruik
Dit proces is belangrijk omdat Youth energy haar klanten bewust wil laten omgaan met hun energie. Om dit te realiseren heeft de klant inzicht nodig in zijn energieverbruik. Dit proces is gekoppeld aan het RPO van het proces “uitlezen van de meter”.

Service verlenen aan klanten
Dit proces is belangrijk omdat Youth energy haar klanten moet helpen als er complicaties zijn voor de klant. Wanneer dit proces stil staat Heeft dit een hoog gevolg voor de reputatie van het bedrijf en is daarnaast ook belangrijk voor de missie van Youth energy.

Advies geven aan klanten
Dit proces is belangrijk omdat Youth energy als missie heeft om een energieleverancier te zijn die de wereld wil verduurzamen. Dit wil ze bereiken door adviezen te geven aan haar klanten. Als het bedrijf haar klanten daarom geen advies kan geven heeft dat impact om het imago van het bedrijf en daarnaast streeft het bedrijf haar missie niet na.

Uitbreiden van klantenaantal
Dit proces is belangrijk omdat youth energie wil blijven groeien om meer winst maar vooral impact in de energiebranche te hebben wanneer dit proces stil staat heeft dat hoge gevolgen op de financiën en de missie van Youth energy.

4. Bussiness continuity plan (BCP)

In dit hoofdstuk zal worden uitgelicht Hoe het bedrijf zal reageren op calamiteiten die de processen stop kunnen zetten.

Dit plan dient regelmatig te worden geëvalueerd en bijgewerkt om te blijven voldoen aan de veranderende behoeften en omgevingsfactoren van het bedrijf. Daarnaast is het belangrijk om regelmatig oefeningen uit te voeren om de effectiviteit van het plan te testen en personeel voor te bereiden op noodsituaties.

4.1 Energie leveren aan klant

Risico's:

- Stroomonderbrekingen of storingen in de energielevering.
- Natuurrampen zoals stormen, aardbevingen, etc.
- Technische storingen in het energienetwerk.

Maatregelen:

- Installatie van back-up generatoren om continuïteit van energielevering te waarborgen tijdens stroomonderbrekingen.
- Regulier onderhoud van energie-infrastructuur om technische storingen te minimaliseren.
- Implementatie van redundante systemen om de impact van storingen te verminderen.
- Monitoring van weersomstandigheden om voorbereid te zijn op mogelijke natuurrampen en daar op te kunnen handelen.

4.2 Uitlezen van de meter

Risico's:

- Technische storingen in het uitleessysteem van de meter.
- Technische storing bij individuele meter van de klant.
- Schade aan meters als gevolg van externe factoren zoals vandalisme, brand, etc.

Maatregelen:

- Periodieke controles en onderhoud van de uitleessystemen om technische storingen te voorkomen.
- Implementatie van beveiligingsmaatregelen om schade aan meters te voorkomen.
- Voorraad van reserveonderdelen om snel te kunnen reageren op eventuele schade aan meters.
- Samenwerking met lokale bedrijven voor snelle reparaties in geval van schade door externe factoren.

4.3 Klanten inzicht geven in energieverbruik

Risico's:

- Technische storingen in de systemen die het energieverbruik bijhouden.
- Onderbrekingen in datatransmissie die toegang tot klantinformatie belemmeren.
- Cyberaanvallen
- Datalekken

Maatregelen:

- Regelmatige controles en updates van systemen om technische storingen te voorkomen.
- Implementatie van redundante systemen voor datatransmissie om onderbrekingen te minimaliseren.
- Klantcommunicatie over mogelijke storingen en alternatieve methoden om inzicht te krijgen in energieverbruik, zoals telefonische ondersteuning.
- Hardening van de database.
- Regelmatig back-ups maken van klantgegevens en opslaan op veilige locatie.

4.4 Service verlenen aan klanten

Risico's:

- Onderbezetting of onbeschikbaarheid van klantenserviceteams.
- Technische storingen die de communicatie met klanten belemmeren.

Maatregelen:

- Implementatie van een back-upplan voor klantenservice, inclusief een noodteam dat kan worden ingezet bij onderbezetting.
- Duidelijke communicatiekanalen voor klanten om problemen te melden en op te lossen, inclusief alternatieve communicatiemethoden zoals sociale media.
- Trainingen van personeel voor crisismanagement en klantenservice in noodsituaties.

4.5 Advies geven aan klanten

Risico's:

- Onderbrekingen in de beschikbaarheid van experts om advies te geven aan klanten.
- Technische storingen die de communicatie met klanten belemmeren.

Maatregelen:

- Ontwikkeling van een virtueel adviesteam dat op afstand kan werken om continuïteit te waarborgen.
- Gebruik van diverse communicatiekanalen zoals e-mail, telefonische ondersteuning en videoconferenties voor adviesgesprekken.
- Reguliere training van adviesteams om up-to-date te blijven met betrekking tot duurzame energieadviezen.

4.6 Uitbreiden van klantaantal

Risico's:

- Onderbrekingen in marketing- en acquisitieactiviteiten.
- Technische storingen die de registratie van nieuwe klanten belemmeren.

Maatregelen:

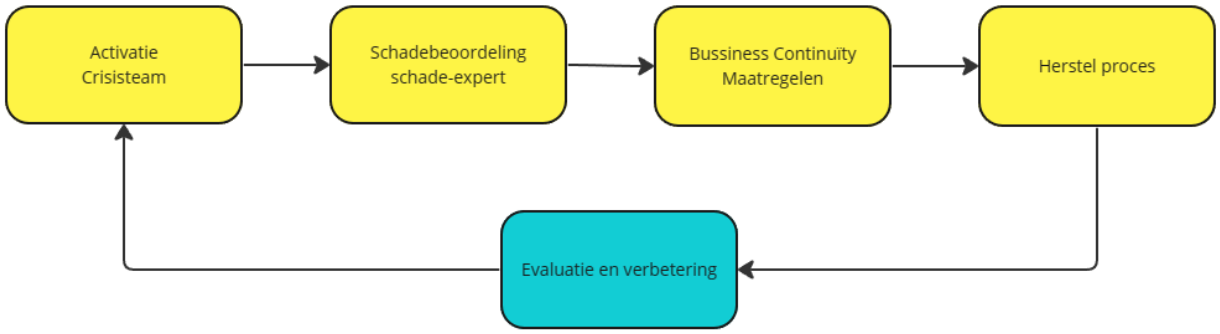
- Diversificatie van marketingkanalen om afhankelijkheid van een enkel kanaal te verminderen.
- Implementatie van een digitaal registratieproces om nieuwe klanten te kunnen blijven werven, zelfs tijdens technische storingen.
- Voorbereiding van een crisiscommunicatieplan om bestaande en potentiële klanten te informeren over eventuele vertragingen in het registratieproces.

5. Disaster recovery plan

In dit hoofdstuk zal worden besproken hoe het bedrijf te werk gaat wanneer er een grootschalige calamiteit heeft plaatsgevonden die belemmering aanbrengt aan het gehele bedrijf.

5.1 Crisisteam & schade beoordeling

In het geval van een calamiteit, zoals een tekort aan personeel, beperkte of geen toegang tot infrastructuur, of een cyberaanval, is het essentieel om onmiddellijk actie te ondernemen om de situatie te beoordelen en te herstellen. Hieronder volgen de stappen die worden genomen met betrekking tot het crisisteam en de schadebeoordeling:



Figuur x: Calamiteiten herstel process.

Boven te zien is het fundamentele proces dat in werking wordt gezet wanneer zich een calamiteit voor doet bij Youth energy. Dit proces wordt ook doorlopen bij trainingen. Na elke training of calamiteit wordt er geëvalueerd op het proces dat zich heeft afgespeeld en daarmee wordt het BCP verbeterd.

Crisisteamactivering:

1. **Identificatie van het crisisteam:**
    - Het crisisteam moet van tevoren worden geïdentificeerd en bestaan uit leden met de vereiste vaardigheden en expertise om snel en effectief te kunnen reageren op noodsituaties.
    - Leden van het crisisteam kunnen onder meer zijn: senior management, IT-specialisten, HR-personeel, communicatiespecialisten en operationele leiders.

Naam	Functie	Telefoonnummer	E-mail adres

2. **Activering van het crisis team:**
    - Bij het optreden van een calamiteit moet het crisisteam onmiddellijk worden geactiveerd volgens de vastgestelde protocollen.
    - Het crisisteam moet bijeenkomen op een daarvoor aangewezen locatie of online platform om de situatie te bespreken, de impact te beoordelen en een plan van aanpak te ontwikkelen.
3. **Taken van het crisisteam:**
    - Coördineren van reacties op noodsituaties en het implementeren van het Disaster Recovery Plan.
    - Communiceren met belanghebbenden over de situatie en de genomen maatregelen.
    - Het nemen van beslissingen met betrekking tot de inzet van middelen en herstelinspanningen.

Schadebeoordeling:

1. **Identificatie van de Schade-expert:**
    - Een schade-expert moet worden geïdentificeerd en opgeroepen om de omvang van de schade als gevolg van de calamiteit vast te stellen.
    - De schade-expert kan intern of extern zijn, afhankelijk van de aard en omvang van de calamiteit en benodigde expertise.
2. **Beoordeling van de Schade:**
    - De schade-expert voert een grondige beoordeling uit van de schade veroorzaakt door de calamiteit, inclusief het evalueren van de impact op personeel, infrastructuur, systemen en gegevens.
    - De schadebeoordeling omvat ook het identificeren van kritieke gebieden die dringend moeten worden hersteld om de bedrijfsactiviteiten te hervatten.
3. **Rapportage en Aanbevelingen:**
    - Na de beoordeling moet de schade-expert een gedetailleerd rapport opstellen waarin de bevindingen, aanbevelingen voor herstelmaatregelen en geschatte herstelkosten worden beschreven.
    - Dit rapport wordt gebruikt door het crisisteam om prioriteiten te stellen en het herstelproces te plannen en uit te voeren.

Door het activeren van het crisisteam en het uitvoeren van een grondige schadebeoordeling kan het bedrijf snel en effectief reageren op calamiteiten en het herstelproces initiëren om de impact op de bedrijfscontinuïteit te minimaliseren.

5.2 Tekort aan personeel

Volgend is een stappenplan dat zal worden gevolgd bij het tekort hebben aan functionerend personeel.

Stappenplan:

1. Identificeer cruciale functies en taken die moeten worden uitgevoerd om de kernactiviteiten van het bedrijf voort te zetten.
2. Stel een lijst op van personeelsleden met vaardigheden die kunnen worden ingezet voor essentiële taken.
3. Plan voor flexibele werkregelingen zoals werken op afstand en het inhuren van tijdelijk personeel om personeelstekorten op te vangen.
4. Train en cross-train personeel voor verschillende taken om flexibiliteit te vergroten in geval van afwezigheid van personeel.
5. Communiceer regelmatig met het personeel over de situatie en bied ondersteuning en richtlijnen voor hun welzijn.

5.3 verminderd/geen toegang tot infrastructuur

Het kan voorkomen, ook al is de kans zeer klein dat een groot gedeelte van de infrastructuur die nodig is voor het uitvoeren van activiteiten wegvalt. Denk hierbij aan bijvoorbeeld een grootschalige brand in het bedrijfsgebouw. Om zo snel mogelijk de functionaliteiten van het bedrijf voort te zetten dient het volgende stappenplan worden gevolgd.

Stappenplan:

1. Test regelmatig de back-up- en herstelprocedures om ervoor te zorgen dat ze effectief zijn in noodsituaties.
2. Identificeer alternatieve locaties of faciliteiten die kunnen worden gebruikt in geval van ontoegankelijkheid van de primaire infrastructuur.
3. Implementeer Cloud-gebaseerde systemen en gegevensopslag om toegang tot bedrijfskritieke gegevens te garanderen, ongeacht de locatie.
4. Ontwikkelprocedures voor het snel herstellen van de infrastructuur, inclusief het opzetten van tijdelijke voorzieningen indien nodig.

5.4 Cyberaanval

Cyberaanvallen zijn steeds meer voorkomend en complexer aangezien informatie van essentieel belang is voor bedrijven en criminele instanties hier veel geld mee kunnen verdienen. Youth energie investeert grondig in informatiebeveiliging aangezien ze niet zonder kan functioneren. Mocht er toch een aanval plaatsvinden van grote schaal dient het volgende stappenplan te worden gevolgd.

Stapopenplan:

Stap 1: Detectie en reactie

1. Wanneer een aanval wordt gedetecteerd, activeer onmiddellijk het crisisteam en start het incidentresponsplan.
2. Het crisisteam Licht de Politie en Autoriteit Persoonsgegevens (AP) z.s.m. in.
3. Isoleer de getroffen systemen en netwerken om verdere verspreiding van de aanval te voorkomen.
4. Verzamel forensische gegevens en bewijsmateriaal om de aard en omvang van de aanval te begrijpen.
5. Communiceer met alle relevante belanghebbenden, inclusief medewerkers, klanten en leveranciers, over de situatie en de genomen maatregelen.

Stap 2: Herstel

1. Beoordeel de omvang van de schade veroorzaakt door de cyberaanval en prioriteer herstelactiviteiten op basis van de bedrijfskritieke functies en systemen.
2. Herstel de getroffen systemen en gegevens vanaf de meest recente back-ups. Controleer grondig en zorgvuldig de integriteit van de herstelde gegevens.
3. Implementeer verbeterde beveiligingsmaatregelen en patches om toekomstige aanvallen te voorkomen.
4. Communiceer regelmatig met alle belanghebbenden over de voortgang van het herstelproces en eventuele wijzigingen in de bedrijfsactiviteiten.

Stap 3: Evaluatie en verbetering

1. Voer een grondige evaluatie uit van de reactie op de cyberaanval, inclusief het identificeren van zwakke punten en lessen die zijn geleerd.
2. Pas het incidentresponsplan en de cyberbeveiligingsmaatregelen dienovereenkomstig aan om de weerbaarheid van het systeem te versterken.
3. Train medewerkers regelmatig over bijgewerkte procedures en maatregelen om hen voor te bereiden op toekomstige noodsituaties.
4. Voer regelmatig oefeningen en simulaties uit om de effectiviteit van het Disaster Recovery Plan te testen en personeel voor te bereiden op noodsituaties.

5.5 Algemene herstelstappen

1. Coördineer herstelinspanningen over alle relevante afdelingen en teams binnen de organisatie.
2. Communiceer regelmatig met belanghebbenden over de voortgang van het herstelproces en eventuele wijzigingen in de bedrijfsactiviteiten.
3. Monitor de situatie na het herstel om ervoor te zorgen dat de operationele activiteiten normaal functioneren en eventuele verdere problemen snel worden aangepakt.
4. Evalueer het Disaster Recovery Plan en identificeer mogelijke verbeteringen op basis van lessen die zijn geleerd tijdens het herstelproces. Pas het plan dienovereenkomstig aan om de veerkracht van de organisatie te vergroten.

6. Data recovery plan

Het doel van dit Data Recovery Plan is om ervoor te zorgen dat de bedrijfskritieke gegevens van het bedrijf veilig worden opgeslagen, regelmatig worden gecontroleerd en getest, en snel kunnen worden hersteld in geval van gegevensverlies of corruptie.

Dubbele locaties voor gegevensopslag:
De bedrijfskritike gegevens zijn op minimaal 2 geografisch gescheiden locaties opgeslagen om te beschermen tegen regionale storingen of calamiteiten.

Regelmatige backups:
Er is een schema ingesteld voor regelmatige back-ups van alle bedrijfskritieke gegevens, inclusief databases, bestanden en configuratiegegevens, om ervoor te zorgen dat alle wijzigingen aan de gegevens worden vastgelegd.

Encryptie van back-ups:
Alle back-ups worden versleuteld om de vertrouwelijkheid en integriteit van de gegevens te waarborgen tijdens opslag en overdracht.

Controle en testen van back-ups:
Regelmatige controles worden uitgevoerd op de back-upprocedures en -apparatuur om ervoor te zorgen dat ze correct functioneren en voldoen aan de vastgestelde normen.

Periodieke testen van de back-up- en herstelprocedures worden uitgevoerd om te verifiëren dat gegevens effectief kunnen worden hersteld in geval van gegevensverlies.

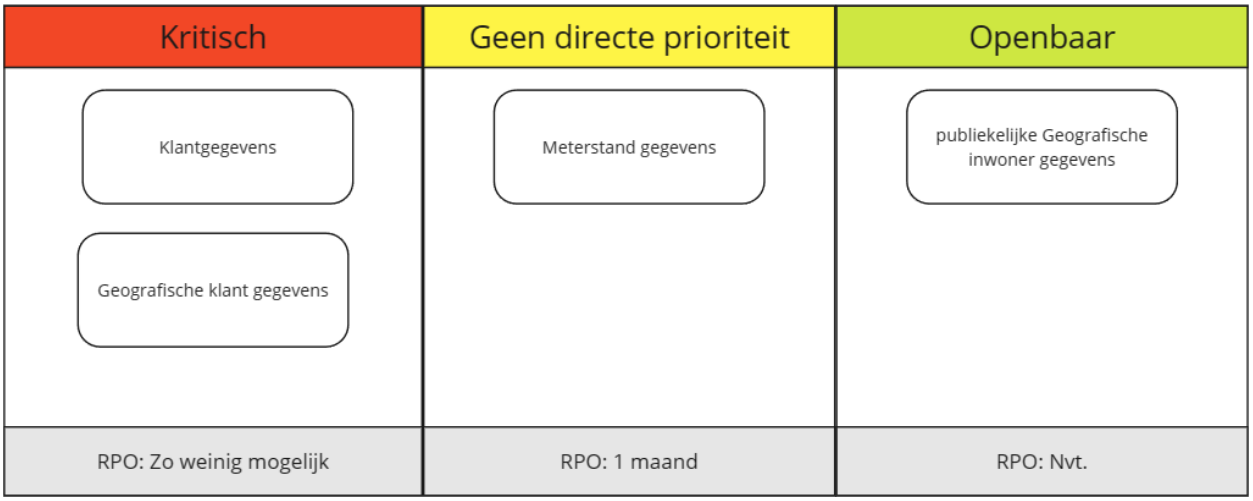
Toegangsbeheer:
De toegang tot back-upgegevens is beperkt tot geautoriseerde gebruikers om ongeautoriseerde wijzigingen of verwijderingen te voorkomen.

De implementatie van deze aspecten in het Data Recovery Plan helpt bij het minimaliseren en verhelpen van verschillende risico's met betrekking tot gegevensverlies of corruptie:

- **Dubbele locaties voor gegevensopslag:**
  - Risico: Regionale storingen of calamiteiten kunnen leiden tot het volledige verlies van gegevens als deze op één locatie worden opgeslagen.
  - Oplossing: Door gegevens op minimaal twee geografisch gescheiden locaties op te slaan, wordt de kans op volledig gegevensverlies aanzienlijk verminderd. Mocht er zich een storing of calamiteit voordoen op één locatie, dan zijn de gegevens nog steeds beschikbaar op de andere locatie.
- **Regelmatige backups:**
  - Risico: Gegevensverlies als gevolg van onverwachte gebeurtenissen, zoals hardware fouten, menselijke fouten of cyberaanvallen, kan leiden tot verstoring van de bedrijfsactiviteiten.
  - Oplossing: Door een schema in te stellen voor regelmatige back-ups worden alle bedrijfskritieke gegevens regelmatig vastgelegd. Hierdoor kan in geval van gegevensverlies snel worden teruggegrepen naar recente back-ups, waardoor de impact van het verlies wordt geminimaliseerd en de bedrijfscontinuïteit wordt behouden.
- **Encryptie van back-ups:**
  - Risico: Ongeautoriseerde toegang tot back-ups kan leiden tot diefstal of manipulatie van gevoelige bedrijfsgegevens.
  - Oplossing: Door alle back-ups te versleutelen, worden de gegevens beveiligd tegen ongeoorloofde toegang tijdens opslag en overdracht. Hierdoor blijft de vertrouwelijkheid en integriteit van de gegevens gewaarborgd, zelfs als ze in verkeerde handen vallen.
- **Controle en testen van back-ups:**
  - Risico: Onbetrouwbare back-upprocedures of apparatuur kunnen leiden tot onvolledige of onbruikbare back-ups, waardoor het herstelproces wordt belemmerd.
  - Oplossing: Door regelmatige controles uit te voeren op de back-upprocedures en -apparatuur wordt ervoor gezorgd dat ze correct functioneren en voldoen aan de vastgestelde normen. Periodieke testen van de back-up- en herstelprocedures verifiëren dat gegevens effectief kunnen worden hersteld in geval van gegevensverlies, waardoor de betrouwbaarheid van het herstelproces wordt gegarandeerd.

- **Toegangsbeheer:**
    - Risico: Ongeautoriseerde wijzigingen of verwijderingen van back-upgegevens kunnen leiden tot verlies of beschadiging van bedrijfskritieke gegevens.
    - Oplossing: Door de toegang tot back-upgegevens te beperken tot geautoriseerde gebruikers wordt de kans op ongeautoriseerde wijzigingen of verwijderingen geminimaliseerd. Hierdoor blijven de integriteit en beschikbaarheid van de gegevens behouden, zelfs in het geval van een beveiligingsincident.

In de volgende afbeelding is de ernst van schade mitigering voor de verschillende informatiebronnen van Youth energy in kaart gebracht.



Kritische informatie:
Deze informatie bevat persoonlijke gegevens van klanten en heeft daarom een zeer hoge prioriteit en mag zo weinig mogelijk verloren gaan. Met name een lek in de klantgegevens kan zeer hoog oplopen in boetes en schade aan het publiekelijk imago van het bedrijf.

Geen directe prioriteit:
De meterstand kan tot aan een maand worden verrekend met de opgeslagen meetdata in de backup van de meterstanden.

Openbaar:
De geografische meetgegevens van inwoners zijn publiekelijk te krijgen via het Centraal Bureau voor de Statistiek (CBS) en als dit verloren raakt bij Youth energie kan het weer opnieuw worden verkregen bij het CBS.

7. Bronnen

Authoriteit Persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/)

Centraal Bureau voor de Statistiek (https://www.cbs.nl/nl-nl)

Digi trust center (https://www.digitaltrustcenter.nl/)

Senesael, (juni 2009) Bussiness continuity management: Handleiding voor implementatie. Geraadpleegd op 28 Maart 2024.

M. Hoogewerf & H. Beerlink, (06-12-2012) Business Continuity Plan GSP. (Versie 1) Geraadpleegd op 28 Maart 2024.