



RDI onderzoekt Business Continuity Management bij netbeheerders voor elektriciteit en gas

Om weerbaar te zijn is het voorkomen van verstoringen en het effectief reageren als er toch een verstoring optreedt belangrijk. Het nemen van maatregelen rondom het herstellvermogen van een organisatie wordt ook wel Business Continuity Management (BCM) genoemd. Bij BCM is het uitgangspunt dat verstoringen zullen optreden, ondanks alle getroffen preventieve maatregelen. Het is met name van belang om de directe impact van de verstoring te beperken en snel te starten met het herstel, om zo de dienstverlening weer op het beoogde niveau te brengen. Een goed ingericht BCM-proces helpt organisaties om adequaat te reageren op (digitale) verstoringen. BCM is sterk gerelateerd aan het incidentproces, waarbij snelle detectie en opschaling naar een crisissituatie van belang.

BCM is met name voor processen die een grote rol spelen in het leveren van de essentiële dienst van belang. BCM begint dan ook bij het in kaart brengen van deze kritische processen en te bepalen waar deze kritische processen van afhankelijk zijn. Denk hierbij aan informatiesystemen en de bijbehorende informatie, personen met cruciale rollen, locaties en de leveranciers. De centrale vraag hierbij is: *Kan voorkomen worden dat bij uitval van een van deze factoren de essentiële dienstverlening grote impact ondervindt?*

Het is van belang dat partijen nadenken over welke continuïteitsmaatregelen nodig zijn om ongewenste impact te voorkomen en als deze impact toch optreedt hoe adequaat gereageerd kan worden (BCM strategie). Vaak is redundantie een goede aanpak om deze impact te beperken. Er zijn echter ook risico's waarbij redundantie niet afdoende is. Denk aan corona waarbij grote groepen medewerkers uitvallen of een ransomware attack die redundant uitgevoerde datacenters gelijktijdig kan raken.

Als er een verstoring met grote impact optreedt, spelen de BCM- en crisismangement plannen een grote rol. In deze plannen staat beschreven hoe de crisisorganisatie eruit ziet en hoe deze zou moeten functioneren. Een belangrijk onderdeel daarbij om een goed beeld te krijgen van de crisis (beeldvorming), welke opties zijn er om in te grijpen en de crisis zo snel in te perken (oordeelsvorming) en hoe kan er een besluit genomen worden (besluitvorming).

Daarnaast worden in dit soort plannen beschreven wat de impact is specifieke maatregelen zoals een uitwijk, terugzetten van een back-up of een alternatieve werkwijze. Door dit al voor een crisis uitgewerkt te hebben zal dit tot een snellere en kwalitatief betere besluitvorming leiden.

In de BCM en crisismangement plannen wordt ook beschreven hoe belangrijke personen en externe partijen bereikt kunnen worden. Crisissen willen nog wel eens buiten kantooruren plaatsvinden, waardoor bereikbaarheid een probleem is. Om te zorgen dat de plannen goed werken is het van belang om periodiek te oefenen omdat het aantal crisissen dat een organisatie doormaakt gelukkig heel laag is.

Resultaten toezicht sector BCM inspecties

In 2022 en een deel van 2023 hebben we voor ons toezicht inspecties over BCM uitgevoerd bij een aantal aanbieders van essentiële diensten. Inspecties hebben plaatsgevonden bij de landelijke en regionale netbeheerders van elektriciteit en gas, inclusief de NAM.

Continuïteit van dienstverlening en het verhelpen van storingen is van oudsher een kerntaak in deze sector. In alle gevallen is dan ook een volwassen en veerkrachtige crisisorganisatie aangetroffen. Het merendeel van de netbeheerders hanteert een BCM methodiek. Hiermee hebben zij inzicht gekregen in hun kritische processen, dreigingen en afhankelijkheden voor de essentiële dienst. Er is binnen de sector ook sprake van BCM certificering maar dit is nog niet standaard.

Alle netbeheerders hebben een business impact analyse uitgevoerd. Een ontwikkelpunt hierbij is de volledigheid van het in kaart brengen van de afhankelijkheden met leveranciers, medewerkers, locaties, informatie en informatiesystemen. Hierbij is het van belang om deze business eisen te vertalen naar eisen voor de interne afdelingen en externe (diensten) leveranciers. De toegenomen complexiteit en digitalisering in combinatie met kortere responsetijden zorgt ervoor dat partijen de keuze maken om niet alle taken meer zelf uit te voeren. Daarmee gaan externe leveranciers een steeds grotere rol spelen.



Vanuit crisismanagement is het oefenen van crisissen en het evalueren hiervan sectorbreed op orde. We zien dat netbeheerders de behoefte hebben om van elkaar te leren en om die reden zijn de overkoepelende resultaten van de BCM inspecties en de aangetroffen best-practises gedeeld in een gezamenlijke sessie met alle netbeheerders.

Wil je als organisatie aan de slag met BCM?

Verkrijg inzicht:

Zorg dat je inzichtelijk hebt welke processen een grote rol spelen in het leveren van de essentiële dienst. Bepaal van welke kritische middelen (informatie/informatiesystemen, rollen, locaties en leveranciers) de kritische processen afhankelijk zijn.

Stel risico's vast en neem maatregelen:

Denk na over welke dreigingen er zijn en met welke maatregelen voorkomen kan worden dat deze dreiging grote impact op de essentiële dienst veroorzaken. Ga aan de slag met de benodigde maatregelen om de continuïteit van de kritische middelen te waarborgen op het moment dat de dreigingen werkelijkheid worden.

Maak plannen om te zorgen dat als er een crisis plaatsvindt, de responsetijd zo kort mogelijk is en dat er maatregelen genomen worden die ervoor zorgen dat de dienstverlening zo snel mogelijk weer op het gewenste niveau is.

Leid op, oefen en evalueer:

Het is eveneens van belang dat medewerkers weten wat van hen verwacht wordt door middel van oefeningen en opleidingen. Oefen periodiek en evalueer deze oefeningen en crisissen om de onderdelen van het BCM te verbeteren. Dit is essentieel om te zorgen dat de maatregelen ook daadwerkelijk functioneren als de nood aan de man is.