Inrichten en onderhouden van een continuïteitsvoorziening

In dit artikel plaatst Ing. Ernst J. Oud (ernstoud@euronet.nl), Senior Consultant bij Getronics Business Continuity BV, calamiteitenplanning in het kader van informatiebeveiliging en beschrijft hij een projectmatige, structurele aanpak voor de inrichting van een operationele continuïteitsvoorziening. Een dergelijke voorziening bestaat uit vooraf te treffen maatregelen en procedures, alsmede de inbedding daarvan in de organisatie. Ook het onderhoud van een dergelijke continuïteitsvoorziening komt aan de orde.

Ondernemingen zijn in steeds grotere mate afhankelijk geworden van informatie en communicatie technologie (ICT). De kwaliteit van de op de markt aanwezige oplossingen voor ICT vraagstukken is veelal dermate hoog dat het gerechtvaardigd lijkt deze systemen voor kritieke bedrijfsprocessen te gebruiken. Toch noemt de Code voor Informatiebeveiliging het proces van continuïteitsplanning een essentiële en fundamentele maatregel; een proces dat elk zichzelf respecterend bedrijf zou moeten implementeren. Klaarblijkelijk verdient dit onderwerp toch nog steeds onze speciale aandacht, ondanks de kwaliteit van aangeboden ICT oplossingen.

Bedrijfscontinuïteit is een breed begrip. De continuïteit van een organisatie is gewaarborgd indien er een winstgevende markt bestaat voor de door de organisatie aangeboden dienst of produkt en indien de bedrijfsprocessen te allen tijde doorgang vinden. De eerste waarborg, de financiele/administratieve continuïteit - het voldoen aan de doelstellingen van de onderneming - is niet het onderwerp van dit artikel. In het navolgende komen die continuïteitsmaatregelen aan de orde die nodig zijn voor de tweede waarborg; het zeker stellen dat de bedrijfsprocessen doorgang vinden ondanks bedreigingen zoals brand, wateroverlast en apparatuurstoring.

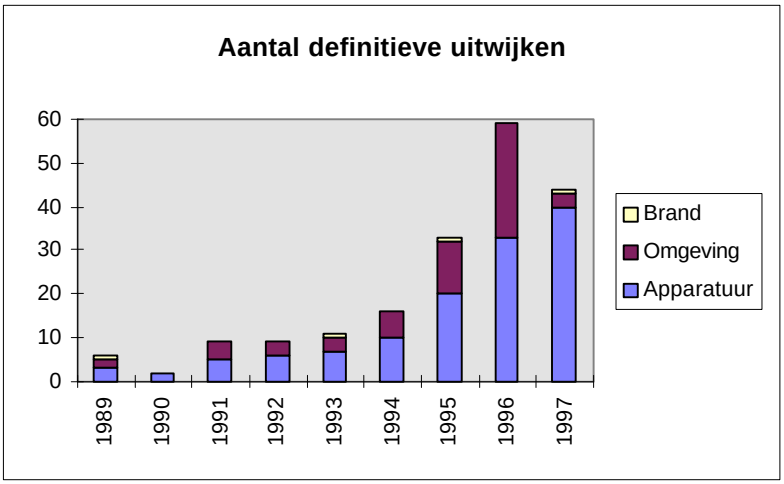
Het optreden van een gebeurtenis welke, bij het ontbreken van passende maatregelen, duidelijk waarneembare gevolgen (materieel dan wel immaterieel) voor de organisatie heeft, noemen we een calamiteit. Het benoemen van deze calamiteiten bij het inrichten en onderhouden van een continuïteitsvoorziening - het stelsel van maatregelen, procedures en organisatorische inbedding teneinde de gevolgen van een calamiteit te beperken - is niet altijd noodzakelijk. In veel gevallen is het definiëren van specifieke calamiteiten welke een onderneming zouden kunnen treffen zelfs een barrière; het heeft het gevaar in zich dat de continuïteitsvoorziening te beperkt opgezet wordt. Voorlopig houden we de term ‘calamiteit’ vast; verderop zullen we zien hoe we deze term voor een specifieke organisatie vastleggen.

Hoewel voor elke organisatie verschillend, is het toch mogelijk een aantal gevolgen van een calamiteit te noemen:

- **Vitale informatie gaat verloren**
- **Financiële controle is niet meer mogelijk**
- **Informatie is niet meer beschikbaar**
- **Goederen en diensten kunnen niet geleverd worden**
- **Demotivatie bij medewerkers**
- **Chaos**
- **Fraude**
- **Faillissement!**

Het is bekend dat meer dan de helft van de bedrijven getroffen door een grote brand binnen drie maanden na de calamiteit niet meer bestaat indien van te voren geen continuïteitsmaatregelen getroffen waren.

Concreet cijfermateriaal laat zien dat de kans op een calamiteit die de bedrijfsvoering bedreigt niet zo klein is als wellicht gedacht wordt. In figuur 1 wordt getoond hoe vaak instanties getroffen worden door een dermate grote calamiteit dat zij de van te voren ingerichte continuïteitsvoorziening moesten aanspreken.



Figuur 1 : Uitwijkmeldingen 1989-1997 bij CUC[1], Lelystad

Van de 1400 klanten die CUC in 1997 kende werden er ruim 40 geconfronteerd met een dermate grote calamiteit dat uitwijk naar Lelystad noodzakelijk werd, bijna 3% dus. Het aantal uitwijkmeldingen per jaar dient uiteraard gerelateerd te worden aan het sterk toegenomen klantenbestand. In het afgelopen decennium blijft het relatieve aantal uitwijkmeldingen min of meer constant rond de genoemde 3%.

Zoals uit de grafiek blijkt is apparatuurstoring de grootste boosdoener. Dit geeft te denken want vrijwel elke afnemer van ICT heeft een servicecontract met de leverancier; klaarblijkelijk bestaat een continuïteitsvoorziening uit meer dan een servicecontract.

Het kader: informatiebeveiliging

Een organisatie die haar continuïteit wil zekerstellen doet er verstandig aan een integraal beleid met betrekking tot informatiebeveiliging te voeren. Continuïteitsplanning in de zin van planning tegen een eventuele calamiteit is namelijk nimmer een op zichzelf staand aandachtspunt. Het heeft relatief weinig zin een perfecte continuïteitsvoorziening in te richten als de risico's op andere aandachtsgebieden binnen informatiebeveiliging factoren hoger liggen.

Een gangbare definitie voor informatiebeveiliging is:

'Informatiebeveiliging is het geheel van preventieve-, repressieve- en herstel maatregelen alsmede procedures welke de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie garanderen met als doel de continuïteit van de organisatie te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald, niveau te beperken.'

[1] Computer Uitwijk Centrum: tot oktober 1998 de bedrijfsnaam van Getronics Business Continuity

Kortom; informatiebeveiliging heeft te maken met garanties en waarborgen, met repressie, preventie én opvang en met procedures naast maatregelen. Volgens de definitie bestaat het inrichten van een continuïteitsvoorziening uit meer dan het treffen van een aantal maatregelen.

Als informatiebeveiliging integraal geïmplementeerd moet worden is het niet nodig het wiel opnieuw uit te vinden, er bestaan namelijk een aantal standaards, zoals:

- **Code voor Informatiebeveiliging (BS 7799)**
- **Voorschrift Informatiebeveiliging Rijksdienst (VIR)**
- **Regeling Informatiebeveiliging Politie (RIP)**

Maar de organisatie kent natuurlijk ook branche voorschriften (Fenit) of de moedermaatschappij stelt eisen en uiteraard stelt de wetgever eisen in de Wet Persoonsregistraties, in de Wet Computercriminaliteit en in de ARBO wet.

De genoemde Code voor Informatiebeveiliging vormt een leidraad voor beleid en implementatie. De Code, uitgegeven door het Nederlands Normalisatie Instituut in Delft, omschrijft in totaal 109 te treffen maatregelen, waarvan er 10 essentieel en fundamenteel zijn; m.a.w. elke organisatie zou ze moeten implementeren.

De 10 essentiële en fundamentele maatregelen zijn als volgt de rangschikken:

Management
- **Toewijzing van verantwoordelijkheden voor informatiebeveiliging**
- **Naleving van de wetgeving inzake bescherming van persoonsgegevens**
- **Naleving van het beveiligingsbeleid**

Procedures
- **Het rapporteren van beveiligingsincidenten**
- **Het proces van continuïteitsplanning**
- **Beveiliging van bedrijfsdocumenten**

Maatregelen
- **Opleiding en training voor informatiebeveiliging**
- **Viruscontrole**
- **Voorkomen van het onrechtmatig kopiëren van programmatuur**
- **Beveiliging van bedrijfsdocumenten**

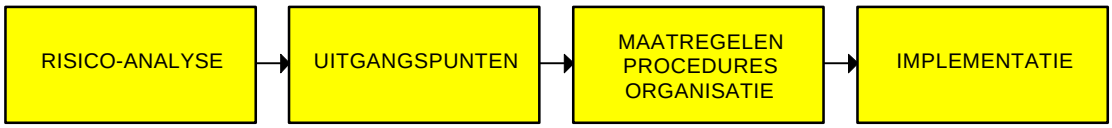
De Code voor Informatiebeveiliging erkent dus dat continuïteitsplanning een essentiële en fundamentele maatregel is.

Continuïteitsplanning; een definitie

Continuïteitsplanning is het van te voren zeker stellen dat de kritische bedrijfsprocessen binnen een bepaalde tijdsduur weer beschikbaar zijn na een (maximale) calamiteit.

De basis voor continuïteit is een continuïteitsplan waarin de onderneming van te voren vastlegt hoe zij haar continuïteit geregeld heeft. Dit roept de vraag op hoe een continuïteitsplan ontwikkeld wordt. De aanbeveling hier is om een in de praktijk bewezen methode te gebruiken en niet zonder meer over te gaan tot implementatie van maatregelen.

Volg een stappenplan en leg de te bereiken doelen vast. De fasen in dit stappenplan zijn bijvoorbeeld als volgt:



Figuur 2 : Een voorbeeld stappenplan

Een voorbeeld van een dergelijke projectmatige methode voor de ontwikkeling van een continuïteitsvoorziening, in gebruik bij honderden bedrijven in Europa, is de Disaster Recovery Methodology™.

Welke methode ook gekozen wordt, cruciaal is dat de keuze van de relevante maatregelen, procedures en operationele inbedding pas mogelijk is na gedegen studie van de bedrijfsprocessen, de risico's en de gevolgen. Deze studie legt de uitgangspunten vast waaraan de continuïteitsvoorziening zal moeten voldoen.

In het hierna volgende wordt, aan de hand van het stappenplan in figuur 2, het inrichten van een continuïteitsvoorziening toegelicht.[2]

Risico-analyse en gevolgschade onderzoek

Voordat de uitgangspunten waaraan de continuïteitsvoorziening moet voldoen bepaald worden, wordt veelal een risico-analyse inclusief een gevolgschade onderzoek uitgevoerd om de risico's voor de bedrijfsprocessen te analyseren. Later worden voor de kritieke bedrijfsprocessen dan de juiste risico's weggenomen of tot een acceptabel niveau beperkt. Wordt deze analyse overgeslagen dan worden maatregelen gekozen welke wellicht het beoogde doel niet waarborgen.

Een *risico-analyse* kan op een aantal manieren plaatsvinden; de meest gangbare is de kwantitatieve methode waarbij de risico's voor het manifest worden van alle onderkende bedreigingen (het optreden van een calamiteit dus) voor de organisatie bepaald worden.

Voor de rijksdienst (ministeries en daaraan gelieerde rijksoverheden) geldt sinds 1994 het Voorschrift Informatiebeveiliging Rijksdienst (VIR). In het VIR wordt de uitvoering van een kwalitatieve Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K analyse) dwingend voorgeschreven. De resultaten van een A&K analyse zijn zeer goed bruikbaar om te bepalen van welke bedrijfsprocessen de continuïteit zeker gesteld dient te worden.

Bij een *gevolgschade onderzoek* wordt de materiële (en wellicht ook de immateriële) schade die optreedt bij het manifest worden van een calamiteit per gebeurtenis gekwantificeerd en worden deze gesommeerd, want

schadeverwachting = Σ (risico x schade)

[2] Merk op dat het inrichten van een continuïteitsvoorziening idealiter plaatsvindt bij het opzetten van de bedrijfsprocessen, hoewel inrichten op een later moment zeker mogelijk is.

Bijvoorbeeld:

Calamiteit	Kans	Gevolgschade	Gevolgschade/jaar
Overstroming	eens per 1250 jaar	ƒ 10.000.000	ƒ 8.000
Brand	eens per 50 jaar	ƒ 5.000.000	ƒ 100.000
Apparatuurstoring	eens per 2 jaar	ƒ 100.000	ƒ 50.000
	Totale	***schadeverwachting/jaar:***	***ƒ 158.000***

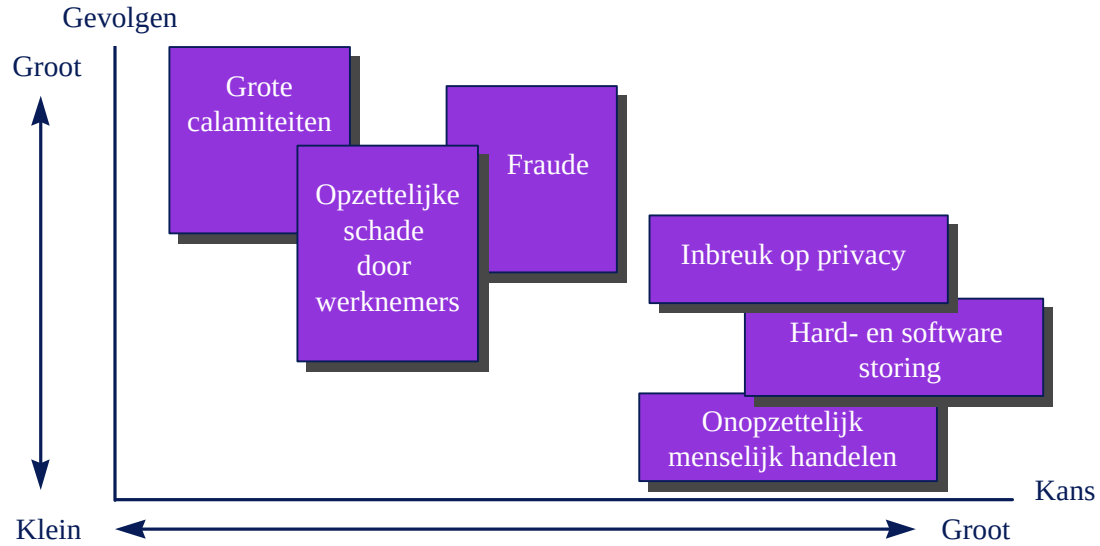
Tabel 1 : Voorbeeld berekening schadeverwachting

De totale schadeverwachting per jaar geeft het management van een organisatie gereedschap in handen om de kosten van een continuïteitsvoorziening de relateren aan de ‘opbrengst’. Echter; dit alles geeft niet meer dan een indicatie, want:

> ***There are three kinds of lies; lies, damned lies and statistics.***
> **Benjamin Disraeli**

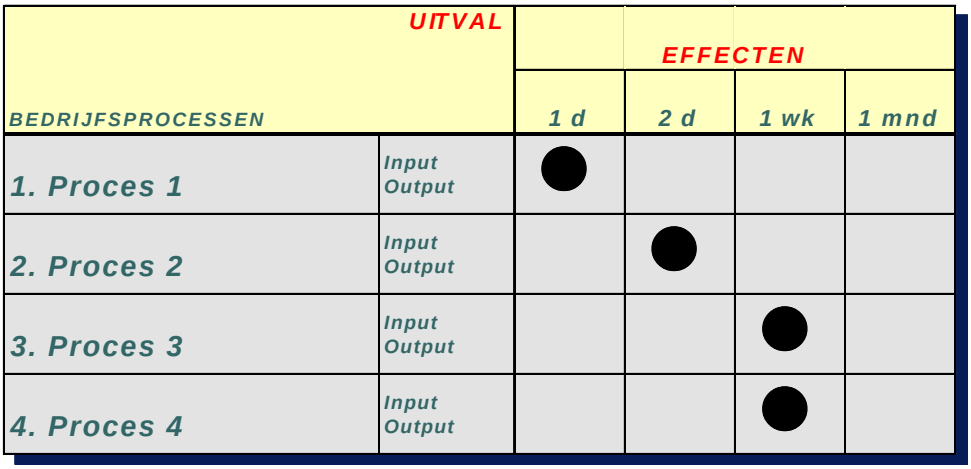
In de laatste jaren komt de kwalitatieve methode meer in zwang. Hierbij worden risico’s niet meer in cijfers achter de komma bepaald maar worden klassen samengesteld en kan het management van een organisatie vervolgens keuzen maken welke klasse(n) calamiteiten men wil kunnen overleven.

Een dergelijke analyse levert bijvoorbeeld het volgende beeld:



Figuur 3 : Kwalitatieve risico-analyse

Deze methode levert meer ‘tastbare’ handvatten. De bedrijfsprocessen worden dan bijvoorbeeld zo weergegeven:



Figuur 4 : De resultaten van een kwalitatieve analyse

Het management van de organisatie ziet hierdoor in een oogopslag welke processen de hoogste prioriteit in een continuïteitsplan dienen te krijgen. Welke methode, kwalitatief of kwantitatief de organisatie ook gebruikt, na de beschreven studies zijn de bedrijfsprocessen geanalyseerd, zijn prioriteiten aangegeven en zijn de risico's onderkend en kan men in principe de maatregelen kiezen (aan de hand van begrippen zoals 'repressief', 'preventief' en 'opvang').

Bijvoorbeeld als volgt:

Actie	**Voorbeeld maatregel**
Niets doen (aanvaarden)	**-**
Preventie (voorkomen)	**Brand-/rookmelding, Toegangsbeveiliging**
Repressie (beperken)	**Brandblusinstallatie, Ontruimingsprocedures**
Verzekeren (afwentelen)	**Materiële gevolgschade polis afsluiten**
Continuïteit (opvangen)	**Computeruitwijk, Calamiteitenplannen**

Het bepalen van de uitgangspunten

Na de risico-analyse start de belangrijkste fase; het bepalen van de uitgangspunten. Wordt deze fase overgeslagen of onjuist doorlopen dan worden later onjuiste continuïteitsvoorzieningen getroffen. Een aantal mogelijke uitgangspunten waar de organisatie over na moet denken:

- **Maximaal Toelaatbare Uitvalsduur (MTU)**
- **Meest ernstige calamiteit waarmee rekening gehouden wordt**
- **Gewenste recentheid van bestanden (maximaal dataverlies)**
- **De prioriteit van de bedrijfssystemen**
- **Het aantal gewenste werkplekken bij een calamiteit**
- **De kwaliteitskenmerken (t.b.v. leverancierselectie)**

Hiervan is de MTU de belangrijkste; hoe lang mogen de tijdens de risico-analyse bepaalde kritische bedrijfsprocessen bij het optreden van een calamiteit, maximaal stil komen te liggen. Met andere woorden; binnen welke tijd dient een continuïteitsvoorziening operationeel te zijn. Op basis van dit soort van te voren bepaalde kencijfers worden de maatregelen, procedures en de organisatie vervolgens ingericht.

Keuze van maatregelen

Voor het bepalen van de benodigde maatregelen moet duidelijk worden welke voorzieningen getroffen moeten worden om de mensen en middelen benodigd voor de kritieke bedrijfsprocessen, bijvoorbeeld op een uitwijklocatie op te bouwen. Aandachtsgebieden zijn:

- **Externe opslag van back-up media**
- **Computersyste(e)m(en)**
- **Datacommunicatie**
- **Uitwijklocatie**
- **Telefonie/fax**
- **Werkplekken**
- **Dealingroom**
- **Mensen**
- **Call center**

Is bekend welke middelen benodigd zijn voor de als kritisch onderkende bedrijfsprocessen dan moet bepaald worden hoe een 'back-up' voorziening voor deze middelen ingericht gaat worden. Dat kan bijvoorbeeld door reserve apparatuur elders op te slaan of door met een goede relatie afspraken te maken. Veelal wordt echter een contract voor een reservering bij een commercieel uitwijkcentrum afgesloten. De bepaling welke kwaliteitskenmerken gelden voor een juiste keuze (denk bijvoorbeeld aan gegarandeerde beschikbaarheid) valt hier buiten beschouwing.

Ontwikkeling van procedures

Als bekend is welke back-up van mensen en middelen van te voren geregeld moet zijn komt een zeer belangrijk aspect aan de orde; het ontwikkelen van de juiste procedures en het inrichten van de organisatie.

De te ontwikkelen procedures worden vastgelegd in het calamiteitenplan.[3]

Een aantal van de te ontwikkelen plannen wordt hierna genoemd, alleen het calamiteitenplan wordt nader toegelicht.

- **Calamiteitenplan**
- **Ontruimingsplan**
- **Aanvalsplan**
- **Veiligheidsplan**

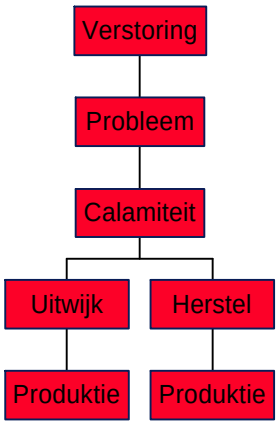
Het calamiteitenplan bestaat uit het escalatieplan en het uitwijkdraaiboek. Deze componenten worden hierna kort toegelicht.

Escalatieplan

Het escalatieplan beschrijft bijvoorbeeld de stappen Probleemherkenning, Calamiteitenbesluit, Uitwijkbesluit en Produktiebesluit en de criteria daarvoor zoals de escalatietijden.

[3] De gangbare Nederlandse term wordt hier gebruikt, hoewel continuïteitsplan een beter begrip is; we plannen immers continuïteit en niet een calamiteit.

Grafisch weergegeven ziet dit er bijvoorbeeld zo uit:



Figuur 5 : Een voorbeeld escalatieprocedure

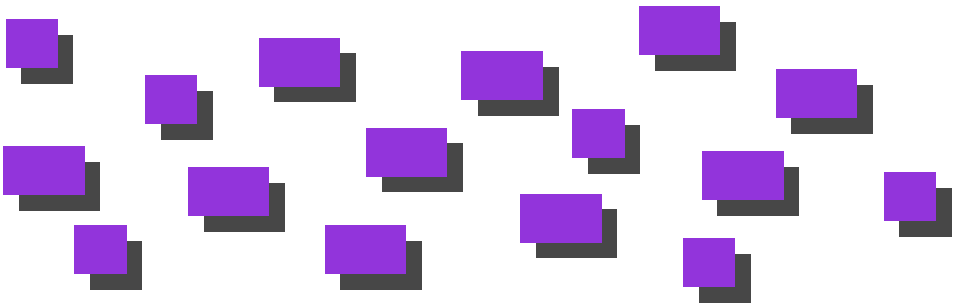
Het is bijzonder belangrijk om het traject van verstoring tot calamiteitenbesluit formeel vast te leggen. Het komt namelijk herhaaldelijk voor dat bij een verstoring in een bedrijfsproces de gevolgen van het uitblijven van een oplossing niet onderkend worden.

Na een bepaalde tijd betekent dit dat de bedrijfsprocessen wellicht gevaar lopen. Als dit niet bewaakt wordt via een formele escalatieprocedure dan blijft men wellicht te lang nadenken over herstel terwijl de uitwijkvoorziening al geactiveerd had moeten worden.

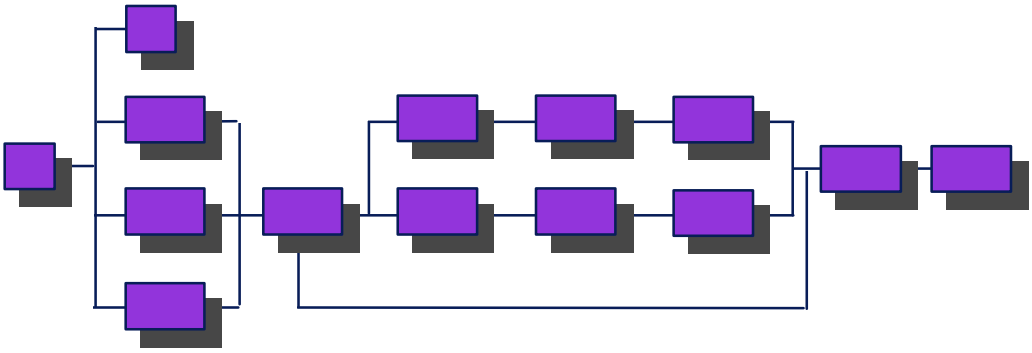
Uitwijkdraaiboek

In het uitwijkdraaiboek worden alle acties in details beschreven om de continuïteitsvoorziening operationeel te maken. Beschreven wordt bijvoorbeeld het opbrengen van systemen, het restoren van de back-up en het herrouteren van netwerkverkeer.

De beste manier voor het opstellen van een dergelijk draaiboek is om middels brainstorm sessies alle activiteiten die uitgevoerd moeten worden te inventariseren. Alle disciplines binnen het bedrijf, betrokken bij de uit te wijken processen, moeten hierin gekend worden. Het gevolg is een groot aantal activiteiten:



Deze moeten vervolgens gerangschikt worden tot een netwerkschema:



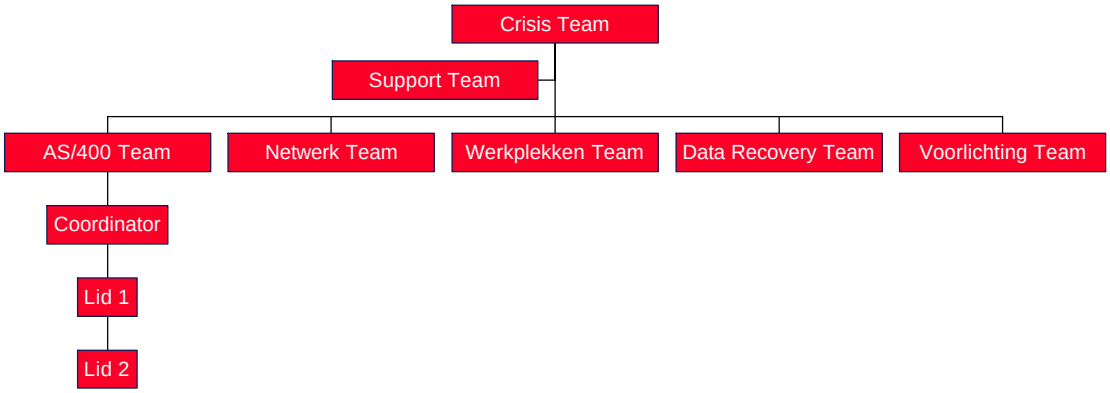
Als elke stap beschreven is dienen ook alle doorlooptijden van de activiteiten afzonderlijk opgenomen worden. Op dat moment is bekend hoe lang dit proces in totaal gaat duren. Komt men boven de maximale tijd uit (de MTU) dan moet men activiteiten parallel gaan laten lopen of moeten anderszins versnellingen aangebracht worden.

Het bovenstaande is geen sinecure; men kan daarvoor het beste gebruik maken van een voor dit doel ontwikkeld tool waarvan er enkele op de markt verkrijgbaar zijn.[4]

Inrichten van een calamiteitenorganisatie

Op het moment van een calamiteit dienen de activiteiten zoals beschreven in het uitwijkdraaiboek uitgevoerd te worden volgens een strak schema.

De daarvoor benodigde personen, veelal ingedeeld in teams, dienen in een ‘slapende’ organisatie (de normale organisatie van een bedrijf wordt vaak de lijnorganisatie genoemd) aanwezig te zijn, bijvoorbeeld als volgt:



Figuur 6 : Een voorbeeld calamiteitenorganisatie

De in de calamiteitenorganisatie aanwezige personen dienen een exemplaar van het uitwijkdraaiboek in hun bezit (liefst thuis!) te hebben en de inhoud er van te kennen.

[4] Een voorbeeld is de DRM Toolkit.

Implementatie

Zonder meer het allerbelangrijkste van het inrichten van een continuïteitsvoorziening op welke wijze dan ook is het uitvoeren van een implementatietest waarbij de getroffen voorzieningen, de procedures en de calamiteitenorganisatie getest worden om zeker te stellen dat aan de uitgangspunten wordt voldaan. Blijkt dit niet het geval dan moet het plan aangepast worden.

Een mogelijke implementatietest is de sloepenrol. Hierbij wordt het totale plan getest; soms zelfs door een calamiteit te ensceneren.

Is met de implementatietest gebleken dat het plan ‘werkt’ dan gaat de operationele fase in. Een continuïteitsvoorziening vergt echter continue aandacht en dient minimaal jaarlijks getest te worden. Mogelijke testen zijn droogtesten (walkthroughs) en audits. Van te voren dienen in een testplan de doelstellingen van de test vastgesteld zijn. Zonder van te voren vast te leggen waar de test aan moet voldoen is het resultaat van de test immers niet aan de verwachting te toetsen.

In de operationele fase moet zeker gesteld worden (bijvoorbeeld door koppelingen met beheersmethodes zoals ITIL change management) dat een verandering in de organisatie of haar middelen verwerkt wordt in het continuïteitsplan. Een continuïteitsplan vergt continue aandacht; een verouderd plan is net zo slecht als geen plan.

Een calamiteit wordt pas een ramp als u niet voorbereid bent!

Een aantal relevante links op het internet

- **Wetgeving**

Arbo wet	**http://www.industriebond.fnv.nl/vgwm/arbowet.html**
Wet Bescherming Persoonsgegevens	**http://www.minjust.nl/c_actual/persber/pb247.htm**
Wet Computercriminaliteit II	**http://www.minjust.nl/c_actual/persber/pb230.htm**

- **Calamiteitenplanning**

Contingency Planning Magazine	**http://www.contingencyplanning.com/index.cfm**
Disaster Recovery Journal	**http://www.drj.com**
Getronics Business Continuity	**http://www.getronics.nl/cuc**
Nationaal Centrum voor Preventie	**http://www.ncpreventie.nl/**
Software voor calamiteitenplannen	**http://www.rothstein.com/data1197/tng050.htm**
Survive!	**http://www.survive.com/**

- **Informatiebeveiliging**

Risico Analyse Tools	**http://www-08.nist.gov/training/risktool.txt**
IB bij de overheid	**http://www.minbiza.nl/acib/**
Nederlands Normalisatie Instituut	**http://www.nni.nl/**