In het themanummer rond continuïteit van Informatiebeveiliging Praktijkjournaal (nummer 6 van afgelopen jaar) was een bijdrage opgenomen van Ernst J. Oud van Getronics Business Continuity waarin een aantal ervaringen bij het aanspreken van een uitwijkvoorziening genoemd werd. Aan het slot van dat artikel werd reeds aangekondigd dat in een volgende uitgave dieper ingegaan zou worden op de beschreven materie. In het navolgende wordt beschreven welke uitgangspunten een organisatie moet formuleren voordat een passende uitwijkvoorziening gerealiseerd kan worden.

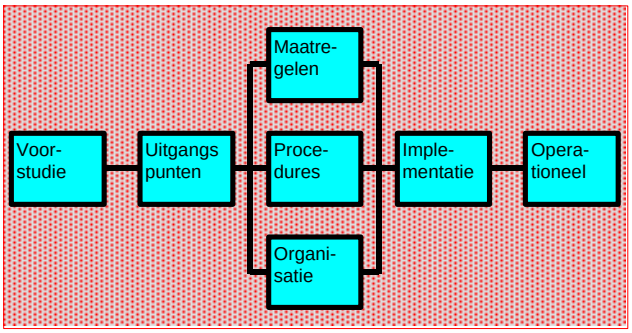
Uitgangspunten voor een uitwijkvoorziening

door Ernst J. Oud

Een operationele uitwijkvoorziening kent drie componenten; de voorzieningen (bijvoorbeeld gerealiseerd in een uitwijkcontract met een commerciële aanbieder), de procedures (zoals een escalatieplan en een calamiteitenplan) en de uitwijkorganisatie (bestaande o.a. uit het crisisteam en de uitwijkteams).

Te vaak wordt een uitwijkvoorziening ingericht zonder dat van te voren de juiste aandacht uitgegaan is naar het formuleren van de uitgangspunten waaraan de uitwijkvoorziening moet voldoen. Door niet goed deze uitgangspunten te beschouwen loopt een organisatie het risico dat bij een daadwerkelijke calamiteit waarbij de uitwijkvoorziening aange-sproken moet worden de uitwijk niet lukt of dat na het opbrengen van de uitgeweken systemen blijkt dat de continuering van de juiste bedrijfsprocessen toch niet mogelijk is.

In het artikel in het themanummer rond continuïteit werd de Disaster Recovery Methodology™ (DRM) reeds voorgesteld. In figuur 1 is ter verduidelijking nogmaals de grafische voorstelling van deze projectaanpak geschetst.



Figuur 1 : Disaster Recovery Methodology™

Zoals uit figuur 1 blijkt, dient de keuze van de juiste maatregelen, de ontwikkeling van procedures en het inrichten van de uitwijkorganisatie, voorafgegaan te worden door een voorstudie waarna pas de bepaling van de uitgangspunten kan plaatsvinden.

De voorstudie

Tijdens de voorstudie worden de bedrijfsprocessen, alsmede de risico's en de gevolgen welke deze processen bedreigen, onderzocht. De voorstudie legt de basis voor het later juist kunnen bepalen van de uitgangspunten waaraan de continuïteitsvoorziening zal moeten voldoen.

De eerste stap van de voorstudie is het bepalen van alle bedrijfsprocessen. Door plenaire sessies met het management van de organisatie worden deze processen geanalyseerd en door business-modelling technieken wordt de informatiestroom en het belang van de diverse processen voor de doelstelling en de output van de organisatie geïnventariseerd.

Tijdens deze analyse wordt duidelijk welke bedrijfsprocessen *kritisch* zijn. In het algemeen zijn dat die bedrijfsfuncties die de 'competitive edge' van de organisatie ten opzichte van de concurrentie waarborgen alsmede de processen waarmee de organisatie haar liquiditeit op korte en lange termijn zeker stelt. Ook worden als kritisch aangemeld die processen welke bij uitval binnen korte termijn tot een niet meer weg te nemen chaos zullen leiden. De diepgang van deze analyse dient niet te worden onderschat. Bij inrichting van een continuïteits-voorziening wordt namelijk in de praktijk te vaak uitgegaan van de IT.

Dit betekent dat bij een uiteindelijke calamiteit IT systemen wel opgebracht kunnen worden maar waarbij dit vervolgens niet leidt tot herstart van bedrijfsprocessen. De organisatie dient dus *vanuit het gezichtspunt van de bedrijfsprocessen* geanalyseerd te worden. Al snel wordt dan bijvoorbeeld duidelijk dat menscapaciteit, logistiek, samenwerking tussen afdelingen, kontakten met toeleveranciers e.d. minstens zo belangrijk zijn dan de IT systemen.

Zijn de kritische bedrijfsprocessen bekend dan dient geïnventariseerd te worden welke mensen en middelen in de ruimste zin benodigd zijn om deze processen uit te voeren en dienen kengetallen rond het volume van input en output bekend te zijn.

Een voorbeeld: *"In het magazijn is het inkomende goederen ontvangstproces kritiek. Dit proces vereist het logistieke computersysteem op twee terminals, drie personen, een fax met telefoonlijn alsmede opslagruimte voor de ontvangen goederen. Het gemiddeld aantal ontvangsten bedraagt 100 per dag resulterend in 250 transacties op het systeem."*

De risico-analyse

Is een duidelijk beeld aanwezig welke bedrijfs-processen bij uitval de organisatie in een kritieke situatie zullen brengen dan wordt veelal een risico-analyse inclusief een gevolgschade onderzoek uitgevoerd om de risico's voor deze bedrijfs-processen te analyseren. Het doel van deze risico-analyse is om in een later stadium *verantwoorde* keuzen te kunnen maken van de te treffen maatregelen. Ook worden de resultaten vaak gebruikt om de baten (in de vorm van gereduceerde kansen) te kunnen wegen tegen de kosten welke gemaakt moeten gaan worden bijvoorbeeld voor een uitwijkcontract.

Tip: In het kader van de milleniumproblematiek is de bovenstaande exercitie soms al uitgevoerd!

De in dat project verkregen informatie kan uitstekend dienen voor een project om een continuïteits-voorziening in te richten of te verbeteren!

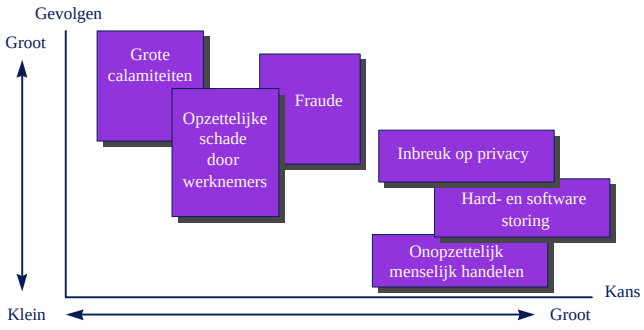
Een *risico-analyse* kan op een aantal manieren plaatsvinden; de meest gangbare is de kwantitatieve methode waarbij de risico's voor het manifest worden van alle onderkende bedreigingen (het optreden van een calamiteit dus) voor de organisatie bepaald worden.

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. De totale schadeverwachting per jaar geeft het management van een organisatie dan gereedschap in handen om de kosten van een continuïteitsvoorziening te relateren aan de 'opbrengst'.

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 2 : Kwalitatieve risico-analyse

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

UITVAL / BEDRIJFSPROCESSEN		EFFECTEN 1 d	2 d	1 wk	1 mnd
1. Proces 1	Input Output	●			
2. Proces 2	Input Output		●		
3. Proces 3	Input Output			●	
4. Proces 4	Input Output			●	

Figuur 3 : 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 vervolgens de uitgangspunten voor de continuïteitsvoorziening gaan opstellen.

De uitgangspunten

Na de voorstudie 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 zijn:

- **De Maximaal Toelaatbare Uitvalsduur (MTU)**
- **De meest ernstige calamiteit waarmee rekening gehouden wordt**
- **De gewenste recentheid van bestanden (dus het maximale dataverlies)**
- **De prioriteit van de bedrijfssystemen**
- **Het aantal gewenste werkplekken bij een calamiteit**
- **De kwaliteitskenmerken (t.b.v. leveranciersselectie)**

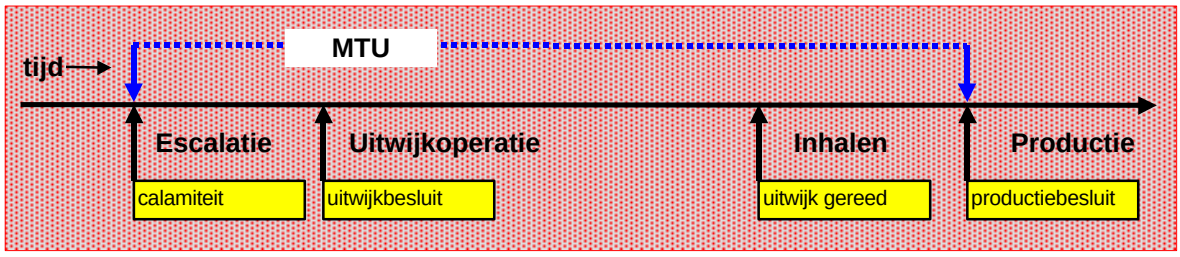
Hiervan is de MTU de belangrijkste; hoe lang mogen de tijdens de voorstudie bepaalde kritische bedrijfsprocessen bij het optreden van een calamiteit, maximaal stil komen te liggen. Met andere woorden; binnen welke tijd dient een continuïteitsvoorziening operationeel te zijn.

Het in de risico-analyse uitgevoerde gevolgschade onderzoek geeft indicaties van de materiële en immateriële financiële verliezen die de organisatie leidt bij uitval. Op basis van deze cijfers is een MTU te bepalen. Echter ook het reeds eerder genoemde optreden van chaos kan de MTU bepalen; soms treden pas duidelijke financiële verliezen op na een uitval van dagen hoewel de organisatie de chaos ontstaan na uitval van enkele uren al niet meer kan corrigeren; dit treedt veelal op bij het verwerken van grote volumes waarbij geen originele gegevens meer voorhanden zijn (zoals de gelduitgifte bij betaalautomaten of bij een dealingroom).

Het mag duidelijk zijn dat een MTU in de orde van uren geheel andere keuzen voor de uiteindelijke uitwijkvoorziening dicteert dan wanneer deze dagen bedraagt. In het laatste geval is verplaatsen van de bedrijfsvoering naar een back-up locatie (zoals een uitwijkcentrum) en het opbrengen van systemen en restoren van databases mogelijk. Bij een korte MTU moet een back-up locatie wellicht volledig schaduw draaien door middel van mirroring technieken. Het juist formuleren van de MTU is dus in een latere fase bij het inrichten van de juiste voorzieningen cruciaal.

In de laatste jaren zien we dat de maximale uitvalsduur steeds verder afneemt. Daar waar in het verleden sprake was van dagen is de tendens nu MTU’s van uren. Een bepaalde MTU betekent overigens niet dat voor de totale uitwijkprocedure deze tijd geldt. Vanaf het moment van het optreden van een calamiteit tot het nemen van het uitwijkbesluit verloopt immers ook tijd en het inhalen van verloren produktie behoort ook binnen de MTU; zie figuur 4.

Naast de MTU is het maximale dataverlies een belangrijk kencijfer. Steeds meer bedrijfsprocessen genereren grote hoeveelheden gegevens in korte tijd. Als deze gegevens bij het weer opbrengen van de kritieke processen absoluut noodzakelijk zijn en de calamiteit waarvoor de uitwijkvoorziening ingericht wordt is dermate ernstig dat beschikbaarheid van de gegevens niet gegarandeerd zal zijn dan dient een extra voorziening (vaker een back-up maken, remote mirroring etc.) getroffen te worden.



Figuur 4 : MTU als totaaltijd

Ook dienen in dat geval ontvangende processen (waar de input data gegenereerd wordt - bijvoorbeeld een frontoffice) fysiek en logisch gescheiden te worden van de verwerking (in de backoffice). Bij een calamiteit is dan 'buffering' van transacties in het ontvangstproces mogelijk als bijvoorbeeld alleen de backoffice getroffen is.

Een continuïteitsvoorziening wordt ingericht voor een bepaalde maximale calamiteit. Voor de keuze van dit uitgangspunt geeft uiteraard de risico-analyse belangrijke informatie. Als de organisatie gevestigd is naast een chemische fabriek dan kan brand, explosie en ontruiming - dus totaal verlies van het pand - een reële maximale calamiteit zijn.

Desalniettemin zijn de cijfers van een risico-analyse niet allesbepalend. Deze geven namelijk alleen de kans aan van het optreden van bepaalde calamiteiten zoals een brand. Het *moment van optreden* van een alles vernietigende brand is echter ook bepalend en kan leiden tot een bijstelling van deze calamiteit als 'worst-case' keuze. Bij een brand overdag, waarbij ook de werknemers bedreigd worden, zijn door verlies van mensenlevens wellicht de bedrijfs-processen niet meer op te brengen. Een andere keuze is dan wellicht passend; doel van de bepaling van dit uitgangspunt is immers om later vast te kunnen leggen over welke materiële en menselijke hulpbronnen ("resources") de organisatie na een calamiteit in ieder geval nog kan beschikken.

Zijn werknemers overigens een bijzonder kritische 'produktie factor', m.a.w. verloren menscapaciteit is bij een zeer ernstige calamiteit niet te over te nemen door bijvoorbeeld uitzendkrachten dan dient de organisatie, ook vanuit haar verantwoordelijkheid voor de werknemers, de resultaten van de risico-analyse en de keuze voor de maximale calamiteit zeer serieus te nemen.

Is een aantal uitgangspunten bekend dan dient men tevens na te denken over de kwaliteitskenmerken welke men aan de in te richten voorziening zal gaan stellen. Denk aan garanties omtrent beschikbaarheid maar ook aan testbaarheid en de benodigde ondersteuning. Een dergelijke lijst kenmerken kan uitstekend dienen voor het selecteren van de juiste partner indien de rest van het project (inrichting van maatregelen bijvoorbeeld door een uitwijkcentrum) uitbesteed wordt.

Uit de inventarisatie van de benodigde mensen/middelen uit de voorstudie kan nu ook het aantal benodigde werkplekken na een calamiteit, het aantal terminals, datacommunicatieverbindingen e.d. gesommeerd worden. Voor al deze hulpmiddelen dient in het vervolg van het project immers een voorziening getroffen te worden.

Op basis van de hierboven genoemde, van te voren bepaalde, uitgangspunten worden de maatregelen, procedures en de (uitwijk)organisatie vervolgens ingericht en na implementatie volledig getest. Dit proces zal in een volgend nummer van Informatiebeveiliging Praktijkjournaal nader uitgewerkt worden.

Ernst J. Oud is senior consultant bij Getronics Business Continuity. In mei is hij voorzitter van een internationaal congres met als onderwerp noodprocedures voor het jaar 2000. Tevens werkt hij in een internationale werkgroep aan het tot stand komen van de vernieuwde ITIL module Contingency Planning. De auteur kan bereikt worden op email adres ernstoud@euronet.nl. þ