Getronics Business Continuity BV (voorheen Computer Uitwijk Centrum BV) is aanbieder van uitwijkservices voor ICT, werkplekken en dealingrooms. Meer dan 500 uitwijksituaties hebben een grote ervaring opgeleverd met alle aan uitwijk verbonden aspecten. In andere publicaties zijn reeds eerder de cases rond de uitwijk van de Crediet- en Effectenbank, Stichting IVIO en Bakker Hillegom gepubliceerd. Het is zinvol eens lering te trekken uit succesvolle aanspraken op continuïteits-voorzieningen bij deze en andere organisaties. In een volgend nummer volgen dan de details.

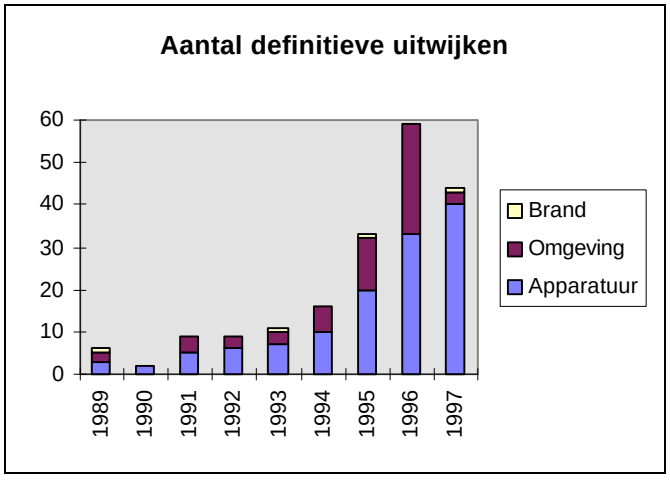
Ervaringen van een aanbieder van uitwijkservices

door Ernst J. Oud

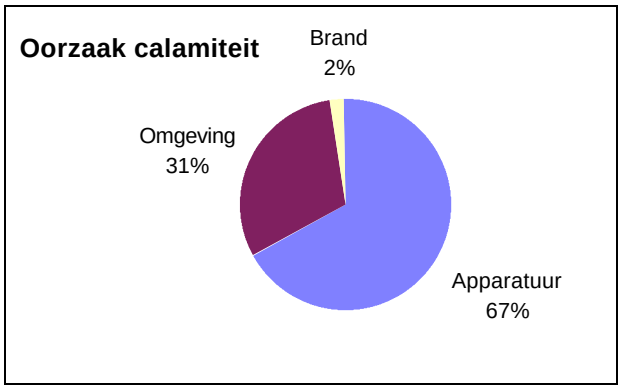
Het inrichten en onderhouden van een continuïteits-voorziening is geen sinecure. Het spanningsveld tussen de statische, slapende back-up voorziening en de dynamische omgeving van veel organisaties lijkt moeilijk te overbruggen maar is dat met de juiste inspanningen echter niet. In het navolgende wordt een aantal ervaringen genoemd waaruit voor elke organisatie leereffecten te behalen zijn.

Uitwijk vaak in andere richting dan verwacht - de redenen voor uitwijk

Bij uitwijk denkt men direct aan het herstarten van gegevensverwerking op een geografisch andere locatie. Dat komt inderdaad in een aantal gevallen voor. Veel vaker daarentegen verhuist de apparatuur van de uitwijk-leverancier naar de klant en niet andersom. Cijfers maken dat direct duidelijk.



Grafiek 1 : Uitwijkmeldingen 1989-1997



Grafiek 2 : Oorzaken van calamiteiten (gemiddeld over 1989-1997)

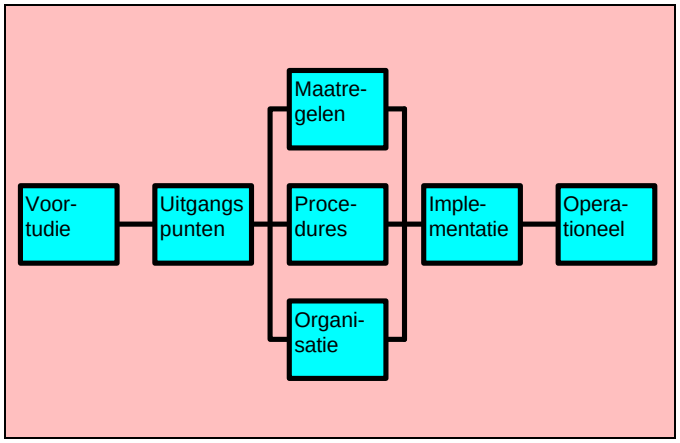
Zoals uit deze grafieken blijkt is apparatuurstoring veruit de grootste reden voor een uitwijk; het betreft hier dan die situaties waarbij de leverancier haar service verplichtingen niet nakomt of een servicecontract ontbreekt. De reservering van de uitwijkconfiguratie kan dan goed van pas komen. Veelal wordt deze apparatuur dan naar de relatie gebracht en aldaar werkend opgeleverd maar bij een vernietigende brand of omgevingsfactoren zoals ontruiming is dit uiteraard geen optie. Uit de grafieken blijkt in ieder geval dat niet te veel vertrouwd moet worden op servicecontracten.

Wordt grafiek 1 gerelateerd aan het klantenbestand van Getronics Business Continuity BV dan is elk jaar het aantal klanten welke geconfronteerd worden met een calamiteit ± 3% van het totaal aantal klanten.

Het genoemde percentage is hoger dan menigeen verwacht en toont aan dat niet altijd alleen de buren met een calamiteit geconfronteerd worden.

Herstarten van bedrijfsprocessen

Succesvolle uitwijksituaties zijn die waarbij (van te voren) uitwijk van *bedrijfsprocessen* geregeld is; veel calamiteitenplannen beschrijven slechts uitwijk van IT-systemen. Leg vast welke bedrijfsprocessen kritiek zijn en welke middelen deze bedrijfsprocessen vereisen en maak *het totale proces* uitwijkbaar. Het benaderen van continuïteitsplanning vanuit de bedrijfsprocessen en niet vanuit IT is niet nieuw; in de Amerikaanse vakliteratuur is reeds langer sprake van de verschuiving van *Disaster Recovery* naar *Business Continuity Planning*.



Figuur 2 : Disaster Recovery Methodology™

De juiste combinatie van maatregelen, procedures en organisatie

Bij het optreden van een calamiteit is het te laat om na te denken over wie wat en hoe moet gaan doen. Ook al is een uitwijkvoorziening (bijvoorbeeld door middel van succesvolle afronding van een DRM™ project - zie figuur 2) van te voren ingericht, minstens zo cruciaal is het vooraf ontwikkelen van een escalatieplan en een uitwijkdraaiboek. Het escalatieplan beschrijft hoe een verstoring in de bedrijfsprocessen leidt tot calamiteiten-, uitwijk- en produktiebesluit. Nog al te vaak ontbreekt een dergelijk plan. Hierdoor loopt een organisatie het gevaar niet tijdig over te gaan tot het uitwijkbesluit waardoor uiteindelijk de maximaal toelaatbare uitvalsduur - een van te voren bepaald cruciaal uitgangspunt - overschreden wordt.

Het uitwijkdraaiboek beschrijft de veelal technische acties welke de uitwijkvoorziening operationeel maken zoals het restoren van de data, het opbrengen van de systemen en het herconfigureren van het netwerk.

Uitwijk wordt soms vergeten

Het lijkt een merkwaardige aanbeveling maar door het ontbreken van een escalatieplan of door het niet bekend zijn van de beschikbaarheid van een uitwijkvoorziening wordt soms geen gebruik gemaakt van de mogelijkheden. Het mag duidelijk zijn dat hierdoor onnodige kosten gemaakt worden. Maak het uitwijkdraaiboek en escalatieplan dus breed bekend in de organisatie.

Het belang van de uitgangspunten

Een uitwijkvoorziening dient te worden ingericht zodat deze past bij de uitgangspunten welke van te voren bepaald zijn, zoals de maximaal toelaatbare uitvalsduur van de bedrijfsprocessen, het maximaal toegestane dataverlies en het aantal benodigde werkplekken in uitwijk. Zonder deze uitgangspunten bestaat er geen fundament voor de uitwijkvoorziening. Toch worden vaak continuïteitsmaatregelen ingericht zonder dat men een duidelijk idee heeft waarom en wat de te bereiken doelen zijn.

Een bijzonder belangrijk uitgangspunt is de maximale calamiteit waar de uitwijkvoorziening voor ingericht wordt. Beperking van de maximale calamiteit (bijvoorbeeld ‘brand op begane grond’) kan betekenen dat uitwijk zinloos wordt (als de brand meerdere etages getroffen heeft). Een te hoog ingeschatte maximale calamiteit (nucleaire explosie) brengt te hoge kosten met zich mee.

Een calamiteit stelt hoge eisen aan de creativiteit van de organisatie

Personeel blijft een beslissende factor; op het moment van de calamiteit wordt hoge aanspraak gemaakt op flexibiliteit en creativiteit.

Plaats personen waarvan zeker is dat zij deze eigenschappen niet hebben dan ook niet in de calamiteitenorganisatie. Het lijkt een automatisme om het crisisteam te laten leiden door de manager van het bedrijf. Toch is dat wellicht niet optimaal.

Operationele uitwijk voor decentrale omgevingen is veelal niet aanwezig

Voor de centrale omgeving (mainframe, mini) is vaak een uitwijkvoorziening en -plan aanwezig. Voor het LAN en andere gedecentraliseerde systemen ontbreken deze veelal vanuit het oogpunt dat deze apparatuur eenvoudig verkrijgbaar is. Die verkrijgbaarheid is evenwel nimmer gegarandeerd. Een continuïteitsvoorziening dient juist garanties te geven; het kan immers uw laatste redding zijn.

Uit een inventarisatie van de bedrijfsprocessen en een risico-analyse blijkt niettemin vaak dat de decentrale systemen en LAN's cruciaal zijn en dus absoluut opgenomen moeten zijn in het calamiteitenplan.

Bewustwording van management vaak nog een probleem

Elke organisatie hoopt van een continuïteits-voorziening geen gebruik te hoeven maken; in die zin is een dergelijke voorziening in wezen een verzekering waarvan de kosten drukken op de winst van de onderneming. Hierdoor is de bereidheid tot investeren soms niet of nauwelijks aanwezig. Een managementsessie waarbij het management samen met een deskundige tot de juiste conclusies komt kan soms zeer verhelderend werken. Het standpunt 'dat gebeurt ons niet' is met eenvoudige middelen af te zwakken. Met een gevolgschade onderzoek is de Return On Investment aan te geven van continuïteitsplanning. Dit maakt de beslissing voor het management inzichtelijker.

Cruciale gegevens vaak niet in externe back-up aanwezig

Keer op keer blijkt weer dat, ondanks een goede back-up strategie, cruciale gegevens, soms zo simpel als de telefoonnummers van inkieslijnen, ontbreken zodat toch de processen niet op te brengen zijn. Zorg er dus voor dat alle middelen, benodigd voor de kritische processen, bekend zijn.

Bij uitwijktesten komt vaak naar voren dat bepaalde informatie absoluut benodigd is maar bij de maximale calamiteit waarmee rekening gehouden wordt niet meer beschikbaar zal zijn. Die informatie moet dan ook elders (bijvoorbeeld in de externe kluis) beschikbaar zijn.

Anekdotisch in dit verband is de systeembeheerder die tijdens een uitwijktest een map tevoorschijn haalde met cruciale instructies voor het opbrengen van de systemen; een map welke altijd op zijn kantoor in de kast stond. De maximale calamiteit was echter totaal verloren gaan van het bedrijfspand. Die informatie moet dus in het calamiteitenplan of in de externe kluis.

Het nut van implementatietest en (jaar-lijkse) uitwijktesten

Het is zeer noodzakelijk om regelmatig te testen of de uitwijkvoorziening en het uitwijkdraaiboek (nog) passen bij de bedrijfsprocessen.

Gebruikt de organisatie IT beheersprocessen zoals ITIL change management probeer dan een koppeling daarmee te realiseren (zie CobiT of Quint Wellington Redwood's IPW); op die manier wordt preventief onderhoud mogelijk.

Is geen formeel beheersproces aanwezig zorg er dan in ieder geval voor dat de voor het calamiteitenplan verantwoordelijke(n) van elke wijziging binnen de organisatie op de hoogte worden gebracht.

Back-up media soms niet beschikbaar

Soms kiest een organisatie voor een externe opslag van de back-up media welke niet 7 x 24 uur beschikbaar is; dat kan leiden tot problemen bij een calamiteit buiten de beschikbare tijd. Het lijkt een open deur maar het advies blijft; kies te allen tijde voor een altijd beschikbare externe opslag.

Effectieve communicatie waardevol

Het melden van het feit dat de organisatie getroffen is door een calamiteit, liefst met vermelding wanneer de bedrijfsprocessen weer functioneel zijn, blijkt de druk van klanten en toeleveranciers enigszins weg te nemen. Zeker als men zich houdt aan de gedane uitspraken is de klantenbinding na een calamiteit zelfs steviger dan daarvoor.

Interne communicatie tijdens een lokale calamiteit is met de moderne mobiele telefoon goed in te richten maar dan moeten de partijen (bijvoorbeeld de coördinatoren van uitwijkteams) elkaars nummers wel kennen! Vermeld deze dus in de uitwijkplannen. Houdt daarentegen bij grote calamiteiten rekening met overbelasting van het GSM net.

"Voorkomen niet altijd goedkoper dan genezen." **Prof. Dr. U. Rosenthal**

Met voldoende aandacht voor de genoemde punten en, na bepaling van de uitgangspunten, een gedegen inrichting van de juiste uitwijkvoorziening, procedures èn organisatorische inbedding is het altijd mogelijk elke calamiteit geen ramp te laten worden.

In een volgend nummer van IB Praktijkjournaal zal verder ingegaan worden op enkele van de genoemde aanbevelingen, met name (in nummer 1/99) op het vereenvoudigen van onderhoud van een calamiteitenplan door koppeling met change management procedures. In de loop van 1999 zal het bepalen van de uitgangspunten waaraan een continuïteitsvoorziening moet voldoen nader aan de orde komen.

Ernst J. Oud is senior consultant bij Getronics Business Continuity. Op dit moment onderzoekt hij de uitwijk van de back-office van een dealingroom bij een grootbank. Tevens werkt hij in een internationale werkgroep aan het tot stand komen van de vernieuwde ITIL module Contingency Planning. þ