Contingency Planning
Universiteit van Amsterdam

B. Eenink – bas@os3.nl
D.J. van Helmond – dirkjan@os3.nl

29 maart 2006

Samenvatting

Veel MKB-bedrijven zijn niet voorbereid op ramp-scenario's die hen kunnen overkomen omdat ze vaak niet genoeg geld hebben of mensen hopen simpelweg dat het hen niet overkomt. In plaats van deze ramp-scenario's de rug toe te keren is het veel veiliger om een aantal kleine maar effectieve voorbereidingen te treffen voor dergelijke rampen. Door een zogeheten contingency plan[1] te maken wordt het een stuk makkelijker voor een bedrijf om na een ramp bedrijfsprocessen te kunnen blijven uitvoeren.

Dit document kunt U gebruiken als handleiding om een contingency plan voor Uw bedrijf op te zetten. Het omvat methodes die algemeen geaccepteerd zijn als bruikbaar en details over hoe U invulling aan deze methode kan geven. Aan het einde van het document staan enkele technische uitdagingen waar een klein bedrijf tegenover kan komen te staan. Vaak moet er dan een afweging gemaakt worden tussen betrouwbaarheid van de oplossing en de kosten. Dit hoofdstuk geeft enkele goedkopere oplossingen aan die geïmplementeerd kunnen worden. Deze halen niet de betrouwbaarheid die een professionele oplossing met zich mee brengt, maar voor een klein bedrijf kan het een wereld van verschil maken.

[1] contingency planning: het plannen van/ voorbereiden op onvoorziene gebeurtenissen

Inhoudsopgave

noot: ICT Continuity planning is een belangrijk proces binnen een bedrijf. Het heeft zelfs een eigen hoofdstuk in de Code voor Informatiebeveiliging (ISO 17799:2005). Een ramp schuilt in een klein hoekje, en als het gebeurt, moet je weten hoe je adequaat in een dergelijke omgeving moet handelen. ICT Continuity is een onderdeel van het veel grotere business continuity planning, wat ook rekening houdt met de liquiditeit van het bedrijf en het hebben van voldoende werknemers om je taken als bedrijf te kunnen uitvoeren. Vanwege de grote omvang van business continuity en de relevantie met het vak *Large Installation Administration* hebben we ons beperkt tot Continuity van de ICT voorzieningen. Een ICT continuity plan werkt niet zonder een compleet bedrijfsomvattend business contibuity plan. Als je besluit om aan continuity planning te beginnen, zorg er dan ook voor dat je het goed doet. Een half continuity plan werkt niet.

1 Inleiding

Veel bedrijven zijn tegenwoordig veel globaler gaan opereren dan vroeger. ICT services en diensten moeten vaak 24x7 voor de klant beschikbaar zijn. Bijna alle ICT diensten zijn afhankelijk van stroom en een internetverbinding als levensbloed in het bedrijf. Een interruptie van deze diensten kan ver-strekkende gevolgen hebben voor een bedrijf. Van eenvoudig verlies van inkomsten door dat er niet verkocht kan worden tot boetes wegens niet nagekomen afspraken of erger, overtreding van wetten. Er spelen zich twee zaken af, ten eerste moet een bedrijf er alles aan kunnen doen om 'up' te blijven. Daarnaast moet een bedrijf nadenken over de actie die ondernomen dient te worden als een onderdeel van de ICT infrastructuur toch plat gaat. Risico management in de vorm van een business continuity plan kan een bedrijf erbij helpen het 'up' houden van services te garanderen. De keuze om een business continuity plan op te stellen kan verschillende oorzaken hebben. Voorbeelden hiervan zijn: noodzakelijkheid vanuit de wetgeving of vanuit verzekeringsoogpunt: Als een bedrijf een business continuity plan klaar heeft liggen wat officieel geaudit is, geven verzekeringsbedrijven vaak korting op verzekeringen omdat een goed business continuity plan kosten van een eventuele ramp drukt.

2 Wat is een BCP nu precies?

Voordat we gaan kijken hoe een Business Continuity Plan in elkaar gezet dient te worden, kijken we eerst even wat een dergelijk plan nou precies inhoudt. Een Business Coninuity Plan is een document waarin alle informatie verzameld is die nodig is om in het geval van een crisis beslissingen te kunnen nemen. Vaak is het business continuity plan geschreven in de vorm van een draaiboek, zodat er op eenvoudige wijze alle zaken stap-voor-stap doorgenomen kunnen worden. Informatie die in een typisch business continuity plan gevonden kan worden omvat ondermeer de policies die in een bedrijf gehanteerd worden. Ook procedures en protocollen hoe gereageerd dient te worden dient in een bepaald detail in een business continuity plan uitgewerkt te zijn. Door deze procedures en protocollen uit te werken, kan een medewerker zonder veel nadenken veel complexere taken uitvoeren omdat er over deze zaken vooraf is nagedacht.

3 Voorbereidingen voor het opzetten van een BCP

3.1 Ondersteuning van Management

Ondersteuning van management voor het opstellen van een business continuity plan is noodzakelijk. Het prettigst zou zijn als er een persoon met beslissingsbevoegdheid in de werkgroep geplaatst zou worden. Tijdens het maken van een business continuity plan kan het mogelijk zijn dat er bedrijfsprocessen anders ingericht zullen worden. Als hier geen druk van management achter staat, kunnen andere medewerkers niet volledige medewerking hieraan verlenen. Hierdoor zal het proces langer duren en meer geld kosten. Daarnaast wordt een business continuity plan ook vaak opgezet vanuit de noodzaak om ISO17799 certificatie te halen. Een dergelijk proces wordt al vaak door management overzien, waardoor aansluiting met het opzetten van een business continuity plan een kleine stap is. Als het proces door management overzien is en tijdens een crisis blijkt dat het business continuity plan niet afdoende is, kan de aansprakelijkheid hiervan ook niet bij een medewerker gelegd worden.

3.2 Inhoud van een Business Continuity plan

Het business continuity plan bestaat uit verschillende onderdelen met ieder hun eigen functie.

Review Mission and Business Functions Het business continuity plan spitst zich toe op het feit dat de belangrijkste services geleverd moeten blijven worden. Dit hoofdstuk wijst de belangrijkste services aan die in het kader van de bedrijfsvoering de meeste waarde hebben voor het bedrijf. Ook wordt er gekeken op welke diensten de services berusten, zodat eventuele afhankelijkheden duidelijk worden.

Business Impact Analysis Dit hoofdstuk bekijkt welke impact een storing in een service voor gevolgen kan hebben. Services en storingen die de grootste impact hebben op de bedrijfsvoering zijn het belangrijkste om te verzorgen. Ook wordt er gekeken of er mogelijkheden zijn om de impact van een storing te beperken door bijvoorbeeld redundancy of policy te wijzigen.

Policies, Procedures and Protocols Dit hoofdstuk bepaald policies, procedures en protocollen die belangrijk zijn in een business continuity plan. Deze documenten komen vaak uit bestaande documentatie binnen het bedrijf. Relevante documenten dienen opgenomen en eventueel aangepast te worden in het business continuity plan.

Written BCP Dit hoofdstuk geeft uitleg hoe een business continuity plan het beste uitgeschreven kan worden, de verschijning van de fysieke vorm van het plan en welke informatie het zou moeten omvatten en hoe het bewaard zou moeten zijn.

Test and Maintain Your BCP Dit hoofdstuk geeft uitleg over verschillende manieren die toegepast kunnen worden om een business continuity plan te testen.

3.3 Opzetten BCP Projectteam

Het opstellen van een business continuity plan kan het beste gedaan worden door een speciaal opgericht team dat zich toespitst op business continuity. Dit team zou de organisatie moeten weerspiegelen zodat uit elk onderdeel van het bedrijf iemand aanwezig is die bekend en ervaren is met de werkwijze, bedrijfsvoering en eventuele problematiek in een bepaalde afdeling. Zo zouden er bijvoorbeeld mensen uit Human Resource, IT, Finance, Management, Legal en Communications in een dergelijk team aanwezig moeten zijn. Het beste zou zijn als een afgevaardigde uit elke afdeling ook beslissingsbevoegdheid zou hebben in de afdeling, zodat in het geval er voor het business continuity plan procedures of policy gewijzigd zou moeten worden dit zonder veel problemen uitgevoerd kan worden.

3.4 Houd medewerkers geïnformeerd

Medewerkers zullen altijd merken dat er veranderingen plaats vinden. Van nature is er altijd weerstand tegen verandering. Informeren vergroot het bewustzijn en de acceptatie van veranderingen. Het is daarom goed om medewerkers bekend te maken met de veranderingen van policy en procedures. Door aan te geven dat de veranderingen plaats vinden in het kader van het veiligstellen van business continuity, en dus ook direct hun baan, zullen medewerkers eerder geneigd zijn om mee te werken aan grote veranderingen. Een voorbeeld kan zijn om een intern memoboard of webpagina bij te houden met de voortgang van het plan en eventuele grote wijzigingen. Wijzigingen binnen een afdeling kunnen intern gecommuniceerd worden middels email.

4 Review mission en business services

Inventarisatie speelt een belangrijke rol bij een ict contingency plan. Een bedrijf moet behalve apparatuur ook een inventarisatie maken van de services welke een bedrijf levert. Voorbeelden van dergelijke services zijn bijvoorbeeld websites hosten, email verkeer afhandelen maar ook (telefonische) helpdesk ondersteuning, afspraken op locatie of bijvoorbeeld stroomvoorziening. Door een lijst van deze services kan een overzicht worden gemaakt welke services de meeste prioriteit hebben en welke services minder belangrijk zijn voor een bedrijf. In geval van een ramp kan een bedrijf dan snel zien welke kritieke services nog operatief zijn en welke aandacht vereisen. In de business h2 planning bestaat hier een begrip voor: "Review mission en business services". Bij een service inventarisatie worden voornamelijk de volgende vragen gesteld:

- Wat zijn mijn belangrijkste services?
- Waar zijn deze services van afhankelijk?
- Wat kan mijn services verstoren?
- Hoelang mogen deze services down zijn?
- Hoe breng ik de services weer up?

In de volgende subhoofdstukken zullen deze vragen tot in detail uitgediept worden om zo inzicht te geven in het opstellen van dit gedeelte van een contingency plan.

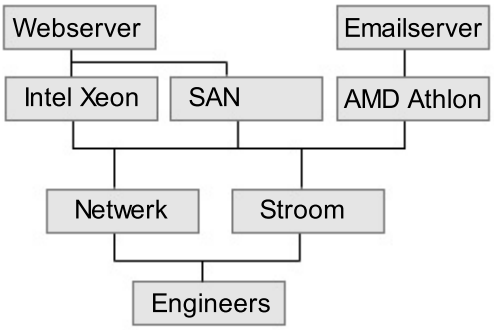
4.1 Wat zijn mijn belangrijkste services?

De belangrijkste services zijn niet eenduidig te noemen, deze lopen uiteen van bedrijf tot bedrijf. Er kan wel een grootste gemene deler gemaakt worden van de definitie van de belangrijkste services voor een bedrijf. Zo zijn belangrijkste services ruwweg in drie typen te verdelen:

- Bedrijfsafhankelijkheden, services waar het bedrijf van afhankelijk is om te kunnen draaien. Hieronder vallen bijvoorbeeld ERP[2] en CRM systemen.
- Financiële afhankelijkheden, services die voor het bedrijf de grootste bron van inkomsten zijn. Hier kan gedacht worden aan helpdesks of webwinkels die afhankelijk zijn van een netwerkverbinding en servers of telefooncentrales.
- Contractuele afhankelijkheden, services die contractueel verbonden zijn aan een bepaalde criteria zoals SLA's[3] of andere gelijksoortige contracten.

[2]ERP: Enterprise Resource Planning, systemen voor bedrijven om voorraadbeheer, boekhouding, personeelsbestanden en dergelijke bij te kunnen houden in 1 pakket

[3]SLA: Service Level Agreement, een afspraak welke service geleverd wordt onder welke voorwaarden



Figuur 1: Voorbeeld van een afhankelijkheidsboom

Deze services moeten daarom voor zover mogelijk altijd geleverd kunnen worden, ongeacht de toestand van het bedrijf. Door de belangrijkste services te destileren kan bij een ramp op deze services geconcentreerd worden om deze als eerste, zo snel mogelijk weer operationeel te krijgen zodat het bedrijf door kan blijven draaien. Het kan erg moeilijk zijn om services prioriteiten te gaan geven. Dit probleem wordt iets duidelijker als er een keuze gemaakt moet worden voor bijvoorbeeld een website met bestellingsfunctionaliteit, email of de telefoonservice waar ook bestellingen geplaatst kunnen worden. Daarnaast kunnen mensen met veel macht persoonlijke belangen voorop gaan stellen in een dergelijke beslissing wat niet ten goede komt van het continueren van de services die wel belangrijk zijn.

4.2 Waar zijn deze services van afhankelijk?

Wanneer er eenmaal een lijst met belangrijkste services is gecreëerd kan er gekeken worden naar de afhankelijkheden van deze services. Het heeft geen zin om er alles aan te doen zodat een service zelf zou kunnen draaien (zoals een webserver) als er bijvoorbeeld geen elektriciteit is waar deze service van afhankelijk is. Door een overzicht van deze afhankelijkheden wordt het snel duidelijk waar nog meer op moet worden gelet bij het maken van een goed contingency plan. Enkele manieren waarop de afhankelijkheden van services duidelijk zichtbaar gemaakt kunnen worden zijn door middel van een tabel of een afhankelijkheidsboom, in het engels ook wel dependency tree genoemd. In zo'n boom staan de diverse afhankelijkheden van een service. Bovenin de boom staan de services en in de knopen eronder staan de services waar ze van afhankelijk zijn en daaronder weer de onderdelen waar die services van afhankelijk zijn etc. In figuur 1 staat een voorbeeld van een afhankelijkheidsboom van een bedrijf met email- en webserverafhankelijkheden. Tegenwoordig wordt de levering van elektriciteit als normaal gezien. In een land als Nederland is dit redelijk goed geregeld maar in Amerika is constante toevoer van elektriciteit helemaal niet zo vanzelfsprekend. Dit terwijl praktisch alle bedrijven 100% afhankelijk zijn van elektriciteit. Vroeger was dit naast gas en stromend water de enige service waar iedereen van afhankelijk was. Sinds enkele jaren is daar een opmerkelijke afhankelijk bijgekomen. Veel bedrijven zijn net zo afhankelijk van internet als van elektriciteit. Deze noodzaak is vooral toe te schrijven

aan de groeiende behoefte aan communicatie. Email is van een speeltje heel vroeger uitgegroeid tot een van de primaire communicatie behoeften van een bedrijf. Daarnaast is ook VoIP, de vervanger van de vaste telefoon in opkomst die ook gebruik maakt van het internet. Waar vroeger twee communicatie netwerken waren, namelijk een telefoonverbinding en een internet verbinding is er nu nog maar een, namelijk het internet. Het telefoon-netwerk is netwerk met een hoge QoS[4] waar dedicated hardware gebruikt wordt om communicatie op te zetten. Het internet wordt voor veel meer doeleinden gebruikt waardoor een dergelijke garantie niet gegeven kan worden. Dit heeft voor bedrijven als gevolg dat ze absoluut niet meer zonder internet kunnen en de internet aansluiting een zeer belangrijke afhankelijkheid is. Temeer omdat sommige bedrijven een internetaansluiting moeten gebruiken om bijvoorbeeld hun ERP systeem te kunnen gebruiken. Bedrijven die meerdere netwerk-afhankelijke services hebben zoals Email, Webinterfaces, Databases moeten hun netwerk in huis onderhouden of ze kunnen ervoor kiezen om de servers in co-locaties neer te zetten of dit volledig uit te besteden aan een derde partij die voor hen de servers beheert en onderhoudt. Bij deze laatste optie worden bedrijfsafhankelijke services minder kritiek omdat het bedrijf kan aannemen dat een derde partij dit afhandelt. Hierdoor kan het bedrijf op andere kritieke services binnenshuis gaan concentreren.

4.3 Wat kan mijn services verstoren?

Nu er een duidelijk overzicht is gemaakt van de belangrijke services voor een bedrijf kan er verder gekeken worden naar de risico's die deze services lopen. Voor elke service moet er een inventarisatie gemaakt worden wat deze service kan verstoren of geheel onklaar maken. Er zijn een aantal verschillende categoriën waarin deze risico's zijn in te delen:

- Geografische oorzaken, waarin vooral natuurrampen voorkomen zoals aardbevingen, tornado's etc
- Technologische oorzaken, alle technische apparaten/ aansluitingen die kapot kunnen gaan zoals kabelbreuken, voedingen die uitbranden etc
- Fysieke oorzaken, lijken op technologische oorzaken met dit verschil dat het mechanische defecten zijn zoals water lekkage, deuren die niet meer open kunnen etc
- Menselijke fouten, alle fouten die door mensen gemaakt worden, de meest onvoorziene fouten

De eerste drie categoriën zijn goed in te schatten. De laatste categorie is vaak het moeilijkst in te schatten omdat mensen onberekenbaar zijn in situaties die ze niet kennen. Er zijn vaak goede voorbereidingen te treffen voor de rampen in de andere categoriën afhankelijk van de hoeveelheid beschikbare middelen. Natuurlijk geldt, hoe meer financiële bronnen er beschikbaar zijn, hoe meer catestrofale gevolgen van rampen te voorkomen zijn.

[4]QoS: Quality of Service, aanduiding om van een verbinding de kwaliteit uit te drukken.

4.4 Hoelang mogen deze services down zijn?

Ondanks alle voorbereidingen kunnen er toch nog situaties voorkomen waardoor services niet continue aangeboden kunnen worden. Soms is het minder erg als services niet continue beschikbaar zijn zolang de gebruikers het maar weten. Gebruikers hebben liever een service die 2 dagen niet beschikbaar is zolang ze ervan weten dan een service die zomaar niet meer werkt omdat ze dan ook niet weten hoe lang het niet meer gaat werken en ongeduldig worden. Bedrijven sluiten met klanten zogeheten SLA's af om uptime van services te garanderen of zo goed mogelijk na te streven. Hierin kan ook beschreven staan hoe lang een service niet bereikbaar mag zijn. Een aantal services zoals webmail hoeft niet 24x7 te werken maar slechts 8x5 of 8x7 zodat er ruimte is voor onderhoud mocht dit nodig zijn. Zolang alles duidelijk afgesproken is (in SLA's) met klanten kunnen bedrijven eventuele schade beperken doordat klanten ook weten waar ze aan toe zijn.

4.5 Hoe breng ik de services weer up?

Als er bij een ramp services niet meer werken zullen deze op een bepaald moment toch weer actief moeten worden. Bij autonome services zal dit vrij makkelijk te realiseren zijn maar een aantal services zal afhankelijk zijn van andere services. Een voorbeeld hiervan zijn servers die wel weer aangezet worden maar met een niet functionerend netwerk zijn de services die de servers aanbieden nog steeds inactief. Bij een inventarisatie moeten de bestaande services ingedeeld worden in klassen van prioriteit om aan te geven welke services als eerst actief moeten zijn voordat andere, afhankelijke services weer geactiveerd worden. Deze klassen zijn niet alleen bedoeld voor fysieke afhankelijkheden zoals logische aansluitingen (de stroom moet eerst aanstaan voordat de server werkt) maar ook voor logische afhankelijkheden zoals een firewall die eerst geactiveerd moet zijn voordat de servers die erachter zitten operationeel mogen worden.

5 Business Impact Analysis

Een engelse definitie van de term Business Impact Analysis:
"Business impact analysis (BIA) is essentially a means of systematically assessing the potential consequences or effects from a various number of business interruptions."
Hier staat in feite dat BIA het volgende inhoudt: een manier om eventuele gevolgen van rampen systematisch af te lopen en te beoordelen wat de risico's voor het bedrijf zijn. Business Impact Analysis oftewel impact analyse is een analyse van de gevolgen die verschillende ramp-scenario's kunnen hebben voor een bedrijf en of een bedrijf in staat blijft om de services te leveren die verwacht worden. Onder de gevolgen valt bijvoorbeeld financiële schade maar ook problemen als imago- of emotionele schade worden hierdoor belicht.

5.1 Financiële kant van impact analyse

Het doel van impact analyse is het creëren van een beeld dat zich concentreert op eventuele kosten bij het down gaan van de belangrijkste services van een bedrijf. Een voorbeeld hiervan is de aanschaf van nieuwe hardware bij het falen van de huidige hardware. Deze kosten zijn meestal een theoretische berekening en soms zelfs een schatting wanneer sommige factoren niet precies bekend zijn. De totale kosten bij een ramp kunnen bestaan uit verschillende onderdelen waarvan sommige minder vanzelfsprekend zijn:

- aanschaf apparatuur
- reparatie apparatuur
- aanklachten
- boetes op grond van SLA's
- overwerk (en daardoor overbetaling)
- ontslagregelingen
- werving nieuw personeel
- onvoorziene uitgaven

Er kunnen nog andere financiële gevolgen zijn voor een bedrijf zoals het niet in staat zijn om diensten te leveren waardoor de inkomsten dalen. Ook kan er een inkomstenverlies optreden door negatieve media-aandacht of het verlies van licenties en rechten.

5.2 Preventie

Voor elk risico dat een service kan lopen om down te gaan worden de zo mogelijk preventieve maatregelen opgesomd, tesamen met de kosten die deze maatregelen met zich mee brengen. Nu zijn bekend: de kosten van een ramp en de kosten van preventieve maatregelen. Deze kosten kunnen tegen elkaar worden uitgezet wanneer de kosten van de ramp nog vermenigvuldigd worden met de kans dat deze ramp optreedt, zie ook figuur 2. Ter illustratie: de kosten

K(ramp)	=	restoratiekosten * P(ramp)
K(preventie)	=	preventiekosten
preventie handig:		K(ramp) > K(preventie)
preventie zeer nuttig:		K(ramp) > 3 * K(preventie)
preventie noodzakelijk:		K(ramp) > 6 * K(preventie)
preventie onhandig:		K(ramp) < K(preventie)
preventie zinloos:		K(ramp) < 3 * K(preventie)

noot: bovenstaande aanbevelingen zijn onofficiële schattingen.

Figuur 2: verhoudingen rampkosten versus preventiekosten

van een orkaan kunnen kolossaal zijn maar de kans dat een orkaan werkelijk langskomt is vrijwel nul. Preventiemaatregelen tegen een orkaan zullen erg duur zijn en omdat de kans dat deze optreedt bijna nul is wordt de noodzaak om een bedrijf hiertegen te beschermen heel erg klein. Andere, meer reële rampscenario's krijgen nu voorrang.

Door de vergelijkingen in figuur 2 te volgen wordt het snel duidelijk welk van de mogelijkheden het voordeligst is voor een bedrijf en of een bedrijf beter preventiemaatregelen kan nemen of niet. Preventiemaatregelen die goedkoper zijn dan de kosten van een ramp hoeven niet altijd beter te zijn voor een bedrijf. Hieronder vallen preventieve maatregelen die op zichzelf wel goedkoop zijn maar waar een correcte werking gehinderd wordt. Hierbij kan gedacht worden aan bijvoorbeeld beveiligingscamera's zonder personeel om de beelden te analyseren. Er zijn veel standaard preventiemaatregelen zoals noodstroomvoorzieningen, dubbel uitgevoerde hardware, extra beveiliging, backups, brandpreventie, uitwijklocaties etc. Afhankelijk van de service waar de preventiemaatregelen voor bedoeld zijn kan het bedrijf beslissen hoeveel de service waard is om deze maatregelen voor te nemen. Als er geen financiële beperkingen zouden zijn zou elk bedrijf zijn infrastructuur liefst vier keer uitgevoerd zien zodat ze altijd op een backup kunnen terugvallen die direct werkt. De realiteit werkt echter anders, door gebrek aan financiële middelen en vanuit een winstoogpunt moet een zo optimale verdeling gevonden worden tussen inkomsten die een service geeft en de kosten die preventiemaatregelen met zich mee brengen. Bij het vinden van een verdeling wordt nauwkeurig rekening gehouden met SLA's en andere afhankelijkheden die aangeven hoe belangrijk een service eigenlijk is en aangeven hoe vaak een service down mag zijn (soms nooit). Fysieke maatregelen op zichzelf zijn niet voldoende. Personeel moet ook getraind en geïnstrueerd worden om om te gaan met bepaalde materialen, apparatuur en/ of handelingen. Dit wordt vaak onterecht als minder belangrijk afgedaan waardoor het op een tweede of nog latere plaats eindigd wat betreft prioriteit in het bedrijf. Toch is training minstens zo belangrijk als de apparatuur zelf. Wat is het nut van een generator als niemand ooit brandstof bijvult?

6 Ontwikkel Policies en Procedures

Een business contingency plan is niet compleet zonder policy ofwel beleid en voorgedefinieerde procedures. Er moeten standaard procedures vastgesteld worden die gevolgd moeten worden in geval van een rampscenario. Hoe belangrijker de service die beschreven wordt in dit beleid, hoe belangrijker is het dat de procedures goed op orde zijn en vervolgens ook nageleefd worden. Dergelijke procedures zijn eigenlijk een specifieke volgorde van handelen afhankelijk van een situatie. Voorbeelden van deze situaties zijn erg uiteenlopend zoals een ontruimingsplan van een gebouw, het uit- en inschakelen van stroom, acties die ondernomen moeten worden na een overval, backups maken/ terugzetten etc. In een ideale wereld zou alles wat gedaan en gemaakt wordt gedocumenteerd worden zodat iedereen ten alle tijden de werking kan opzoeken van een stuk soft- of hardware. In de praktijk valt dit erg tegen. Gestandariseerde procedures zoals een vluchtplan van een gebouw zijn vaak wel in orde, mede omdat het wettelijk verplicht is. Zodra er gekeken wordt naar een ICT afdeling komt het voor dat er vaak eigen programma's of scripts gemaakt zijn om bepaalde taken te vergemakkelijken. Door gebrek aan tijd of interesse wordt hier vaak geen of gebrekkige documentatie voor gemaakt. Wanneer een rampscenario zich voltrekt wordt pas duidelijk dat er onverwacht een behoorlijke afhankelijkheid is ontstaan van de toen nog werkende scripts. Na een ramp kan het door gebrekkige documentatie moeilijk tot onmogelijk zijn om dergelijke functionaliteit weer volledig terug te krijgen.

6.1 Bestaande interne documentatie

Interne documentatie van een bedrijf houdt alle documentatie in die gemaakt is en het beleid wat van hogerhand is opgelegd. Deze documentatie kan als basis dienen voor een business contingency plan. Een business contingency plan is nog uitgebreider omdat hier behalve gebruiksaanwijzingen en bijvoorbeeld brandplannen, duidelijke procedures in moeten staan die stap-voor-stap helder beschrijven wat er moet gebeuren. Deze documentatie moet regelmatig gecontroleerd en eventueel bijgewerkt worden zodra er de documentatie verouderd blijkt. Dit kan komen door aanschaf van nieuwe apparatuur maar ook door een veranderende omgeving. Een voorbeeld hiervan is een verbouwing waardoor een bepaalde (vlucht-) deur niet langer bestaat. Bijhouden van documentatie kost veel tijd en daarmee geld. Dit is vaak niet beschikbaar omdat er geen tastbare reden gegeven kan worden waardoor dit werk prioriteit krijgt. Het is iets vaags wat ooit een keer handig kan zijn als er misschien iets gebeurt. Vaak heeft personeel het zelf ook veel te druk met meer concrete taken die voltooid moeten worden en de documentatie "komt wel een keer". Niet dus. Toch is er op het moment van een ramp helemaal geen tijd om rustig uit te vinden wat er gedaan moet worden. Mensen kunnen in een crisis situatie vaak niet meer helder nadenken door paniek. Een plan met duidelijke stappen is dan een uitkomst omdat dan alleen een lijst gevolgd moet worden zonder na te hoeven denken. Vaak blijkt de noodzaak van een dergelijk plan pas acheraf als het kwaad al is geschied. Zoals al eerder genoemd is er zeer weinig tijd en geld beschikbaar in een bedrijf maar eigenlijk zou iedere werknemer direct documentatie moeten ontwikkelen of aanvragen zodra deze een belangrijke

De standaard, ISO 17799	www.17799central.com/holland.htm
Voorbeeldplannen	web.mit.edu/security/www/pubplan.htm
Overheidshandleiding	www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf
Algemene voorbeelden	www.contingencyplanning.com
Lokale gemeente plannen zoals brandweer, politie etc	

Figuur 3: Bronnen voor Business contingency planning

handeling moet verrichten waarvan niet duidelijk bekend is hoe deze uitgevoerd moet worden of waarvan documentatie verouderd is. De term "belangrijke handeling" is een vrij breed begrip maar werknemers zouden dit begrip moeten opvatten als een handeling waarvan zij denken dat het op welke manier dan ook te maken heeft met hun eigen veiligheid op en om de werkvloer. Op deze manier kan een contingency plan zonder al te veel werk toch bijgehouden worden en in niet al te grote bedrijven is dit een goede manier om een dergelijk plan zelfs op te bouwen.

6.2 Bestaande externe documentatie

Behalve interne documentatie van een bedrijf zijn er nog meer bronnen om kennis uit te vergaren. Hoewel een business contingency plan een bedrijfsgericht plan is bestaan er wel degelijk onderdelen die vrij algemeen zijn. Er bestaat veel open documentatie over risk management en contingency planning waardoor deze onderdelen al een keer goed uitgedacht zijn. Het is dan ook raadzaam om niet opnieuw te proberen het wiel uit te vinden maar bestaande plannen te lezen en hiervan de nuttige onderdelen te gebruiken voor het bedrijf. Enkele bronnen staan in Figuur 3. Veel bestaande business contingency plannen zijn zeer geschikt om als basis te dienen voor een eigen plan, zeker als het plan uit een bedrijf komt wat qua structuur overeenkomt met het eigen bedrijf. Plannen voor gemeente diensten en andere open instanties zijn vaak al goed uitgedacht en publiek inzichtelijk dus het is zonde om dat zelf nog een keer te gaan uitvinden met alle tijd en kosten van dien.

6.3 Ondersteunende documentatie

Behalve plannen voor het bedrijf en procedures van hard- en software moet er ook ondersteundende documentatie beschikbaar zijn. Hierbij moet gedacht worden aan uitgeschreven taken en verantwoordelijkheden van personeel en secundaire contactmogelijkheden zoals telefoonnummers waarop kritieke verantwoordelijken 's nachts bereikbaar zijn etc. Deze documentatie moet goed verspreid en bekend worden onder personeel omdat iedereen moet weten wat er moet gebeuren in geval van een ramp. Ook een belangrijk onderdeel van documentatie zijn plannen van het gebouw en verdiepingen, unieke kamernummers in combinatie met telefoonnummers en een inventarisatie van welke apparatuur in welke ruimtes staat. Met een dergelijke lijst is het veel makkelijker om te bepalen wat er waar mis gaat en wat er aan gedaan kan worden. Afhankelijk van het kennisniveau van medewerkers kunnen er verschillende lagen gemaakt worden van hetzelfde plan. Een illustratie maakt dit wat duidelijker:

- Een receptioniste die kennis heeft van kamer- en telefoonnummers van alle medewerkers.
- Een conciërge die kennis heeft van kamernummers en de architectuur van stroomaansluitingen in het gebouw.
- Een hoofd ICT die kennis heeft van de indeling van alle apparatuur in ruimtes en waar welke server staat.
- Een IT specialist die kennis heeft van de IP adresserings schema's van alle servers en netwerk routes.

Met een beschikbare lijst van medewerkers en hun verantwoordelijkheid kan er in geval van een ramp een procedure worden opgesteld met wie wanneer contact opgenomen moet worden om bepaalde problemen op te lossen. Dit voorkomt dat er ten tijde van een ramp nog nagedacht moet worden over wie nou eigenlijk de sleutel heeft tot de toegang van de meterkast.

6.4 Informatie beleid

Wat niet onderschat moet worden is een beleid met procedures voor inlichtingen. Wanneer een ramp zich voltrekt zullen er binnen de kortste keren media en andere geïnteresseerden aankloppen voor informatie. Het is van cruciaal belang dat een bedrijf juiste informatie verstrekt aan media en personen met andere belangen in het bedrijf zoals aandeelhouders, klanten, leveranciers en niet te vergeten de medewerkers zelf. Zo kan een beleid worden opgesteld waarin vaststaat wie de media inlicht, wie de klanten inlicht etc. Er staat in wat er verteld wordt, en welke informatie wel en niet bekend mag worden. Als een deel van een bedrijf afbrand is het voor de financiële situatie en continuëring van het bedrijf behoorlijk belangrijk dat iedereen weet of dit een leegstaande ruimte was of een ruimte die primitieve services van het bedrijf verzorgde. Vooral de media heeft een belangrijke invloed. Zodra de media incorrecte feiten vermeld zullen veel geïnteresseerden een verkeerd beeld krijgen van de situatie van het bedrijf. Het komt ook voor dat media eigen verhalen verzinnen of de situatie behoorlijk aandikken waardoor een bedrijf veel negatiever in het nieuws komt. Zelfs hiervoor zou een bedrijf een procedure moeten hebben om direct correcte informatie te kunnen verschaffen, bijvoorbeeld middels persberichten.

6.5 Restore voorbeelden

Wanneer een ramp zich voltrekt wil een bedrijf zo snel mogelijk door kunnen gaan met het werk wat gedaan moet worden. Hierbij is het van belang dat een service die onderbroken is zo snel mogelijk weer operationeel is. Door regelmatig backups te maken, zowel volledige backups als incrementele backups, zal er zo min mogelijk data verloren gaan bij een ramp. Het is verstandig om ook zogeheten offsite backups te hebben, backups die fysiek op een andere plaats liggen. Belangrijke data kan, mits niet te groot, in plaats van op trage backup media zoals tapes opgeslagen worden op usbsticks of andere universele media. Hierdoor kan een bedrijf kritieke gegevens snel op praktisch elke plek inlezen en gebruiken. Waar niet zo snel aan gedacht wordt maar wat heel nuttig kan

zijn, zijn primitieve middelen om een onderbreking van een service bekend te maken. Een voorbeeld hiervan kan een statische webpagina zijn met een storingsmelding, een persbericht of zelfs een telefoongesprek. Wanneer een goede reden gemeld wordt voor de onderbreking zullen klanten en/ of gebruikers het probleem eerder begrijpen en minder snel geneigd zijn ongeduldig te worden. Met weinig inspanning is het mogelijk om klanten een indicatie te geven over de tijd die de downtime nog gaat duren. Wanneer dit een realistische benadering is zal dit niet tot onnodig boze gebruikers en/ of klanten leiden. Naast backups met data is het handig om werkplekken van gebruikers beschikbaar te kunnen hebben. Als een ruimte met werkplekken bijvoorbeeld is afgebrand zou het kunnen helpen om medewerkers tijdelijk thuis te kunnen laten werken. Op deze manier kan er toch gewerkt worden en de werkplekken in het bedrijf kunnen hierdoor ook snel weer worden opgebouwd. Zoals al eerder gemeld is moet er een hardware inventarisatie gemaakt worden maar ook software inventarisatie is heel belangrijk. Het voorbeeld van de scripts zonder documentatie is heel toepasselijk. Als enkele grote paketten zoals SAP gebruikt worden zal hiervoor documentatie bestaan en men weet dat dit gebruikt wordt. Een software inventarisatie is nodig om juist die scripts waar een grote afhankelijkheid van is opgebouwd te documenteren en beschikbaar te kunnen maken in geval van een ramp. Wanneer een bedrijf kritieke services zo snel mogelijk in de lucht wil hebben kan het zeer nuttig zijn om goedkope hardware achter de hand te hebben om tijdelijk deze services zo snel mogelijk op te laten draaien. Gebruikers zullen het erger vinden als een service zoals DNS niet draait dan wanneer het vier keer zo langzaam draait omdat er het tijdelijk draait op een desktop 2 Ghz PC. Dan draait het tenminste en kan er gebruik gemaakt worden van deze service. Met een creatieve geest kan een heel eind gekomen worden; als een gebouw ontruimd moet worden zal een simpele helpdesk met klapstoeltjes in een weiland net zo goed werken als wanneer iedereen netjes in een gebouw achter een bureau zit, bij een beetje goede uitvoering merkt de klant hier namelijk vrij weinig van.

7 BCP Vastleggen in een document

Als een business continuity plan eenmaal is opgesteld moet het vastgelegd worden. Een ideale vorm om een dergelijk plan vast te leggen is in de vorm van een draaiboek. Een draaiboek kan gebruikt worden om in geval van crisis elke procedure stap-voor-stap uit te voeren. Dit heeft als voordeel dat mensen die tijdens een crisis vaak overhaast handelen niets over het hoofd zien. Daarnaast kan het draaiboek ook dienen als centrale plaats voor alle benodigde informatie tijdens een crisis. Er moet dus goed na gedacht worden over de samenstelling van dit draaiboek. Als het draaiboek compleet is, moet het ook op een dermate manier gedistribueerd zijn dat het op het moment dat het benodigd is, ook gebruikt kan worden, wat betekent dat de juiste mensen op de juiste tijd hierover moeten kunnen beschikken.

7.1 Samenstelling draaiboek bepalen

Door het draaiboek een duidelijke en chronologische volgorde te geven, geeft dit houvast aan de uitvoerenden tijdens de crisis situatie. Tijdens deze situatie moeten ze het draaiboek kunnen vertrouwen. Het testen van het draaiboek is daarom ook erg belangrijk. Dit hoofdstuk geeft enkele onderdelen aan waarbij rekening gehouden dient te worden of deze opgenomen zouden moeten worden. Niet elk onderdeel is benodigd voor elke situatie. Belangrijke infomatie zoals informatienummers, alarmcodes en telefoonnummers van de directie moeten bij elkaar geconcentreerd zijn. Het is ook mogelijk om voor verschillende functies de samenstelling van het draaiboek te wijzigen, zodat bijvoorbeeld een manager geen draaiboek met technische details heeft, en een engineer geen draaiboek met allerlei bedrijfskundige informatie. Ook blijft de verspreiding van geheime informatie op deze manier beperkt. Het beperkt ook de tijd die iemand nodig heeft om zijn specifiek benodigde informatie op te zoeken.

Een pen Elk draaiboek zou een pen bijgevoegd moeten hebben. Tijdens crisis moeten continue aantekeningen gemaakt worden. Op een dergelijk moment moeten eenvoudige zaken zoals het zoeken naar een pen voorzien zijn. Een pen kan bijv. in de rug van een ringband geschoven worden of met een touwtje aan de kaft vast gemaakt.

Leeg papier Om aantekeningen op te kunnen maken. Zorg voor een paar lege paginas en een paar belijnde paginas aan het begin en aan het einde van het draaiboek.

Duidelijke chronologische inhoudsopgave Een uitvoerder moet tijdens crisis snel de informatie kunnen vinden die voor hem van belang is. Een duidelijke inhoudsopgave in chronologische volgorde kan hierbij helpen. Door de chronologische volgorde van het draaiboek hoeft er niet continue gebladerd te worden, zodat een uitvoerder zich meer op de uitvoering kan concentreren.

Kleurcodering van bladzijdes Door verschillende onderdelen in het verslag vast te leggen op verschillende kleuren papier, bijvoorbeeld rood voor technische documentatie, geel voor controle functies en groen voor

telefoonnummers etc, kan de zoektijd terug gebracht worden als iemand op zoek is naar specifieke informatie.

Policies Policies moeten aanwezig zijn in het draaiboek. Het liefst in een vereenvoudigde vorm met keyword index. Als er een keuze gemaakt moet worden, kan op deze manier snel gekeken worden of aan de bedrijfspolicy voldaan wordt met een bepaalde oplossing. Dit is voornamelijk belangrijk in omgevingen waar door de wet gereguleerd wordt, zoals bijvoorbeeld met persoonsgegevens.

Procedures Herbouw van services moet volgens vastgelegde procedures verlopen. Als een engineer een service moet starten, moet hij duidelijkheid hebben over de uit te voeren stappen. Als op een dergelijk moment deze keuzes gemaakt moeten worden kunnen er fouten in het proces optreden.

Kritieke volgorde De volgorde waarin services gerestored worden moet vastgelegd worden. Op deze manier kom je niet in de problemen met afhankelijkheiden van services van elkaar. Vervolgens kunnen ook de meest bedrijfskritische applicaties als eerste weer gestart worden. Een indeling als 'critical, essential, important, non-critical' zou bijvoorbeeld ingevoerd kunnen worden.

Communicatieplan In het moment van crisis zullen veel mensen in een bedrijf behoefte hebben naar informatie. Naar medewerkers die niet aanwezig zijn moet de staat van het bedrijf en eventuele gevolgen gecommuniceerd worden. Personen met belangen in het bedrijf moeten gerust gesteld worden en de media moet geïnformeerd worden met feiten. In het geval dat communicatie naar deze groepen achter blijft, kan er gespeculeerd worden en dat kan sommige bedrijven meer schade opleveren dan de daadwerkelijke ramp zelf.

Benodigd Personeel Inventarisatie Voor elke werkzaamheid die gedaan moet worden volgens het plan moet een indeling gemaakt worden hoeveel personen met welke kwalificaties benodigd zijn. Hierdoor kan snel een werkgroep voor elke taak samengesteld worden.

Inventarisatie ICT Omgeving Het draaiboek moet een recente inventarisatie omvatten van de benodigde hard- en software. Indien er nieuwe apparatuur besteld moet worden, weet men direct welke apparatuur en welk type benodigd is.

Mijlpaal Overzicht Om de voortgang van de restore te kunnen volgen zouden verantwoordelijke personen een overzicht met mijlpalen in hun plan moeten hebben. Hierbij kunnen ze bijhouden hoever ze zijn met de restore operatie. Ook kan deze informatie bruikbaar zijn bij communicatie naar derden en media. Voor elke service dient minimaal één mijlpaal aanwezig te zijn. Indien services opgedeeld kunnen worden dient er voor elke onderdeel een deelmijlpaal te zijn.

Veiligheidsmaatregelen Een restore operatie mag geen nieuwe problemen of veiligheidslekken introduceren. Zorg ervoor dat belangrijke zaken

zoals veiligheidsvoorschriften, maar ook firewall policies opgenomen zijn in het business continuity plan.

Deze onderdelen zouden algemeen beschikbaar moeten zijn in een business continuity plan. Voor elk bedrijf kan specifieke informatie benodigd zijn. Ga dit na en zorg dat ook deze informatie in het plan verschijnt.

7.2 Distributie BCP

Als het business continuity plan eenmaal op papier staat moet het gedistribueerd worden zodat alle personen die het nodig hebben er op de juiste tijd bij kunnen. Zo zou elke medewerker die een taak heeft in het plan een draaiboek in bezit moeten hebben. De plaats waar deze medewerker zijn plan opslaat moet duidelijk gemaakt worden. Zo is het niet de bedoeling dat deze plannen allen op het bedrijf bewaard worden. Een medewerker kan deze plannen beter thuis bewaren. Op het moment dat er een ramp gebeurt waarbij het gebouw verloren gaat, zijn de plannen bewaard gebleven. Op het bedrijf dienen kopieën aanwezig te zijn voor algemeen gebruik. Daarnaast is het aan te bevelen om kopieën in de buurt buiten het gebouw op te slaan. Eventueel kan ook nog een digitale versie op een onafhankelijke plaats op Internet opgeslagen worden, zodat er altijd versies bijgeprint kunnen worden. Indien het business continuity plan informatie bevat die geheim moet blijven is het verstandig om de opgeslagen variant op een veilige plek weg te zetten.

8 BCP testen

8.1 Het doel van testen

Het testen van het business continuity plan is erg belangrijk om vast te stellen of de juiste maatregelen zijn genomen. Er zijn verschillende manieren waarop het business continuity plan getest kan worden. Hypothetisch, in een vergaderzaal, per onderdeel of in totaal. Per situatie en per afdeling moet gekeken worden wat de beste methode is om deze tests te laten plaatsvinden.

Doelen die nagestreeft dienen te worden bij testen:

Vaststellen of redundante systemen functioneren Indien je preventieve maatregelen hebt genomen, dien je ook vast te stellen of deze preventieve maatregelen functioneren op de bedoelde manier. Een dergelijke test kan vaak niet hypothetisch gedaan worden. Vaak kan een test in een testomgeving voldoende uitsluitsel geven. Indien de werkelijke situatie complexer is dan de testsituatie, dient het aanbeveling om ook in de live omgeving een test uit te voeren.

Controle of policies en procedures volledig zijn Policies en procedures moeten in een testomgeving nagelopen worden om na te gaan of alle zaken afgedekt zijn. Een dergelijke test is moeilijk om in de werkelijkheid te testen. Het is daarom verstandig om deze test hypothetisch uit te voeren. Pijnpunten in de afhandeling van scenario's kunnen vastgelegd worden en naderhand verwerkt worden in het business continuity plan. Deze tests dienen regelmatig uitgevoerd te worden om twee redenen. Mensen die tijdens een crisis een belangrijke rol hebben, hebben zo alvast geoefend met verschillende scenario's. Daarnaast komt het regelmatig voor dat procedures en polcies veranderd worden binnen een bedrijf. Hier kan tijdens een dergelijke test op ingesprongen worden door het plan tijdig aan te passen.

Controle of alle data beschikbaar is Deze test kan altijd uitgevoerd worden. Er zijn twee manieren om te testen of alle data veilig is. Je kan een zeer uitgebreide en tijdrovende test doen door alle data van alle tapes terug te zetten, of je kan er voor kiezen om bijvoorbeeld wekelijks een willekeurig bestand van een willekeurige server te restoren. Het voordeel van de eerste test is dat je zeker weet dat je al je data terug kan halen. Het nadeel is echter dat het veel tijd kost. De tweede test kost aanzienlijk minder tijd, maar je hebt ook minder zekerheid of al je data veilig is. Als je de tweede procedure enkele maanden hebt uitgevoerd gaat de betrouwbaarheid van de tweede test wel sterk omhoog.

Nagaan of communicatie plaats vindt Deze test is erg moeilijk uit te voeren. Mensen communiceren in crisis-situaties altijd anders dan in reguliere situaties of testsituaties. Een goede manier is om de communicatietest te piggy-backen op een andere test. Zorg ervoor dat bepaalde auditors tijdens de testen vooral de communicatie in de gaten houden. Dit kan bij zowel de hypothetische tests als de testen met delen of de test voor de hele live omgeving.

8.2 Voorbereidingen op testen

Informeer je medewerkers dat er een test plaats vindt. In het geval van een volledige test zullen de meeste medewerkers wel hinder ondervinden van de test. Geïnformeerde medewerkers zullen hiervoor begrip kunnen opbrengen. Ook voorkom je hierdoor dat ongeïnformeerde medewerkers of beheerders taken gaan uitvoeren die de resultaten van de test kunnen beïnvloeden, zoals bijvoorbeeld onderhoudswerkzaamheden aan de backupvoorziening of de redundante apparatuur. Zorg ervoor dat je je medewerkers vodoende informatie geeft zodat ze ook zelf een inschatting kunnen maken wat de invloed zal zijn op hun werkzaamheden. Meld onder andere wat voor test op welk onderdeel uitgevoerd zal worden, de locatie en het tijdstip waarop de test zal plaatsvinden, het scenario dat gebruikt zal worden en eventuele beperkingen die gelden tijdens het uitvoeren van de tests, zoals bijvoorbeeld het verbieden van onderhoud aan redundante of backup systemen. Ook kan een onderdeel van de test zijn om bepaalde mensen uit te sluiten van deelname aan de test om te kijken tot welke mate overige medewerkers bepaalde taken kunnen overnemen.

8.3 Verschillende soorten tests

Hypothetische tests Een hypothetische test omvat het testen van een business continuity plan in de hoofden van de verantwoordelijken tijdens een ramp. De test kan gehouden worden in een vergaderruimte waar afgesproken is in theorie een specifiek scenario uit te voeren. Een hypothetische test is bruikbaar om de volledigheid van een business continuity plan te testen. Procedures kunnen worden doorgenomen alsof een crisis zich werkelijk voordeed, waarbij de verantwoordelijke personen volgens de policy zouden moeten handelen. Mensen raken zo bekend met het plan en kunnen in het geval van een werkelijke crisis efficiënter optreden. Tijdens deze testen zouden waarnemers aanwezig moeten zijn die controleren of alle procedures volledig nagelopen worden en dat mensen volgens de policy handelen.

Component tests Een component test is een test die in de werkelijke omgeving wordt uitgevoerd, maar waarbij slechts een gedeelte van de procedures getest wordt. Dit kan en bruikbare methode zijn als een deel van je infrastructuur in gebruik is en geen storing mag ondervinden, of als het test team niet groot genoeg is om alle procedures en een keer te testen. Het is wel van belang dat in het geval van component tests er toch wordt nagegaan wat de relatie en impact is op de omliggende infrastructuur, zodat in een echte crisis-situatie deze gedeeltelijke proceduretests geen onbekende problemen introduceren. Ook kunnen gezamelijke tests worden uitgevoerd, bijvoorbeeld een data-restore test terwijl een gedeelte van het netwerk onbereikbaar is.

Volledige tests Een volledige test is de beste manier om een business continuity plan te testen. Een volledige test kijkt naast het volledig zijn van de procedures en policies ook of ze bruikbaar zijn in een crisis-situatie. Helaas omvat een volledige test vaak veel tijd en medewerking van alle personeelsleden. Ook kan de impact van een test dermate groot zijn

dat het onmogelijk is om een dergelijke test uit te voeren. Toch is het verstandig om minimaal een keer per jaar een grote crisis te simuleren. Dit is de enige manier om er zeker van te zijn dat het plan duidelijk en volledig genoeg is om bruikbaar te zijn in crisis-situaties. Een mogelijkheid die de impact in zekere zin terug brengt is de test uit te voeren in een testomgeving. Vaak kan dit problemen wel aan het licht brengen, maar complexe problemen inherent aan de infrastructuur blijven hiermee onbelicht. Tijdens een volldige test is het wel mogelijk om erachter te komen of de communicatie tussen verantwoordelijke personen voldoende is om de crisis te bezweren.

8.4 Test Evaluatie

Na het uitvoeren van een test moet een analyse plaats vinden. Elke medewerker die aan de test heeft meegedaan zou individueel ingelicht moeten worden. Wat ging er goed tijdens de test, wat ging er fout en wat verdient verbetering? Met een groep analisten zou elke functie, elke policy en elke procedure nagegeken moeten worden of deze volledig uitgevoerd is. Zo niet, dan moet nagegaan worden waar dit aan lag. De resultaten van deze analyse moeten gebruikt worden om het business continuity plan bij te werken.

8.5 BCP periodiek bijwerken

Naast het bijwerken van het business continuity plan als gevolg van de tests is het ook belangrijk om periodiek de huidige business goals opnieuw vast te stellen en een nieuwe impact analyse uit te voeren. De situatie waarin een bedrijf opereert kan veranderen. Een bedrijf kan zich toeleggen op nieuwe services en nieuwe producten. Als het plan niet is aangepast op de nieuwe situatie kan er niet optimaal gebruik van gemaakt worden. Tijdens deze periodieke evaluatie dient er gepraat te worden met risk managers. Eventueel kan hierbij hulp gevraagd worden van externe bedrijven die gespecialiseerd zijn in risk management.

9 Business Continuity en het MKB

In het MKB wordt vaak veel minder aandacht besteed aan business continuity management. Dit heeft twee oorzaken. Het MKB wordt veel minder gereguleerd dan grote concerns. Niet aandeelhouders maar de ondernemer zelf is vaak degene die de grootste schade ondervind van bedrijfsinterrupties. Hierdoor gelden veel regels met betrekking tot bedrijfsvoering niet voor deze grote groep bedrijven. Omdat de ondernemers niet verplicht zijn adequate maatregelen te nemen om hun bedrijfsvoortgang zeker te stellen, schieten deze maatregelen er vaak bij in. Een tweede oorzaak is dat business continuity management voor midden- en kleinbedrijven vaak investeringen in tijd, geld en mankracht kost die deze bedrijven niet beschikbaar hebben. Dit hoofdstuk behandeld enkele problemen waar een midden- of klein bedrijf tegenaan kan lopen en mogelijke work-arounds die een bedrijf kan implementeren om de benodigde service toch te kunnen blijven bieden. Vaak leunen deze work-arounds op redundante services van toeleveranciers zoals Internet-Providers en Telefonie aanbieders. Zo kan de impact bij een ramp gereduceerd worden.

9.1 Contingency voorzieningen Huisvesting

Bij een ramp zoals het afbranden van een bedrijfspand, kan het werk compleet stil komen te liggen. Een zeer kosteneffectieve en redelijk goed te implementeren work-around voor dit probleem kan begeleid worden door het opstellen van een 'thuis-werk' beleid. Bijna iedereen heeft thuis een computer. Als het mogelijk gemaakt kan worden om de meest belangrijke interne services thuis ontsloten kunnen worden op een eenvoudige manier kunnen medewerkers vanuit hun eigen huis hun taken voort zetten. Een duidelijk beleid kan bijvoorbeeld zijn dat medewerkers middels een webapplicatie bij hun email en belangrijke bedrijfsdocumenten kunnen. Telefonie kan middels een gsm van de zaak die automatisch het doorkiesnummmer van het bedrijf bij de telecom operator wordt doorgeschakeld.

9.2 Contingency voorzieningen Email en Website

Preventie tegen rampen door middel van redundancy is kostbaar. Een tweede server, netwerkverbinding of misschien wel een complete uitwijklocatie is soms een investering die het MKB niet kan maken. Voor belangrijke services die extern bereikbaar moeten blijven, zoals je webservice en email kan je een fallback server installeren en plaatsen bij een bedrijf dat colocatie ruimte verhuurt. Op een dergelijk moment is je mail niet meer direct beschikbaar voor al je medewerkers, maar derden waar je contact mee hebt merken er in ieder geval niets van. De website (eventueel gevuld met statische informatie) blijft beschikbaar, en mail ook zal niet *bouncen*. Daarnaast kunnen deze diensten vaak ook ingekocht worden bij grotere Internet Service Providers.

9.3 Contingency voorzieningen External Networking

Connectiviteit met Internet is voor veel bedrijven tegenwoordig noodzakelijk. Kleine bedrijven die business ADSL gebruiken voor hun internet connectiviteit kunnen in het geval van een netwerkstoring middels een ISDN-2

verbinding een backup verbinding opzetten. Middels intelligente QoS mechanismes kan de belangrijkste dienst, bijvoorbeeld email, voorrang gegeven worden op de verbinding. Een dergelijke oplossing is geen vervanging voor een 8 mbit ADSL verbinding, maar kan wel zorgen dat niet-realtime systemen met een beperkte bandbreedte behoefte geen probleem ondervinden van de netwerkstoring. Grotere bedrijven met bijv. een snellere Internetverbinding, bijvoorbeeld meer dan 50 mbit, kunnen een breedband ADSL verbinding als backup nemen. Deze backup verbinding gaat vaak via een ander pad dan de primaire verbinding, waardoor de beschikbaarheid niet van de zelfde factoren afhankelijk is. Ook hierbij kan QoS gebruikt worden om het belangrijkste verkeer voorang te geven, zodat bedrijfskritische processen geen of minimale overlast ondervinden bij een beperkte bandbreedte.

9.4 Helpdesk

In een contingency situatie zal door veel medewerkers een beroep gedaan worden op de helpdesk. Gebruikers die vanuit huis werken kunnen vaak sommige resources niet bereiken. Hulp bij gebruik in het geval van webapplicaties of VPN verbindingen is noodzakelijk voor gebruikers die uit hun dagelijkse omgeving gehaald worden. Een tweede probleem is dat veel van je helpdesk medewerkers vaak bezig zijn het contingency plan uit te voeren. Hierdoor is er een onderbezetting op de helpdesk. Toch is het noodzakelijk om de helpdesk bezet te houden. Zet ook veel informatie in publiek bereikbare plaatsen zoals bijv. een FAQ op internet. Een helpdesk medewerker kan in sommige gevallen gebruikers naar deze FAQ verwijzen om eenvoudige problemen door de gebruiker zelf te laten oplossen. De meer zelfstandige medewerkers die begrijpen hoe het systeem in elkaar zit, kunnen tijdelijk toegewezen worden aan de helpdesk om zo de helpdesk te ondersteunen bij eenvoudige problemen. Bij grote problemen kan het niet altijd lonend zijn om alle medewerkers te helpen. Doel moet zijn om de belangrijkste mensen en vervolgens de grootste groep mensen aan de gang te krijgen.

9.5 Backups

Het maken van goede backups is een van de belangrijkste taken binnen een contingency plan. Bij het maken van een backup kan er gekozen worden of er een backup van de data wordt gedaan, of een backup van het complete systeem inclusief het besturingssysteem. Bij veel grote bedrijven kan een nieuwe server uitgerold worden waar alleen de data wordt terug gezet waarvan een backukp is gemaakt. Als je een klein bedrijf hebt, kan het practischer zijn om het besturingssysteem in de backup mee te nemen. Hierdoor kan bij een restore een werkende omgeving in één keer terug gezet worden. Het is verstandig een externe backup drive achter de hand houden. Zo weet je zeker dat je gehuurde apparatuur kan gebruiken om een backup terug te zetten.

9.6 Configuration Management en Computer verhuur

Het bijhouden van de wijzigingen in je IT omgeving is een erg belangrijke zaak. Als je in een crisis beland, wil je duidelijk hebben wat wel en wat niet aanwezig is in je netwerk. Configuration Management kan een grote taak zijn

en daarom wordt dit bij veel bedrijven vaak niet gedaan. Als je toch een eenvoudige vorm van configuration management opzet, heb je in geval van een crisis een duidelijk overzicht van de apparatuur die je gebruikt en wat je hiervan eventueel verloren bent. Indien je computer en netwerkapparatuur moet huren om je tijdelijke infrastructuur weer te starten, hoef je in ieder geval geen overzicht te maken van de benodigde apparatuur. Dit scheelt weer in tijd die je beter kan gebruiken om een noodsituatie op te bouwen. Probeer ook om alleen maar standaard apparatuur in je netwerk op te nemen. Op aparte apparatuur zit vaak langere levertijd. Als je al je backups bij de hand hebt om een systeem te restoren, maar je hebt geen hardware om op te restoren, kun je je netwerk nog niet her-opbouwen. Ook in het belang van het aanwijzen van je kritieke services is het belangrijk om een overzicht te hebben welke apparatuur afhankelijk is van andere apparatuur. Dit kan eventueel ook duidelijk worden uit de Configuration Management Database want dat kan er ook in aangegeven worden.

9.7 Tools

Bij het bouwen van een nood-netwerk kunnen veel fouten optreden omdat niet alle beslissingen volledig doordacht genomen zijn. Het is daarom belangrijk om een notebook met daarop systeem en netwerkanalyse tools achter de hand te houden. Minimale tools zoals traceroute, nmap, ethereal, telnet en ssh zouden aanwezig moeten zijn. Het liefst een complete linux distributie zoals Auditor of STDknoppix. Het voordeel van deze distributies is dat deze op een LiveCD verkrijgbaar zijn. Een administrator kan zijn eigen notebook gebruiken voor het booten van deze CD. Fysieke tools zoals schroevedraaiers of een kabeltester zou een administrator ook bij de hand moeten hebben. Daarnaast zijn er enkele omgevingen waar specifieke tools voor nodig zijn zoals bijvoorbeeld inbus sleutels of ander speciaal gereedschap.

9.8 Automatische installatie

Een backup-unattended-installatie-omgeving kan een kostbare uitgave zijn. Vaak kan deze omgeving vereenvoudigd worden door ISO's of images van je meest gebruikte besturingssystemen op een bootable cd te branden samen met een uitvoerbaar programma zoals bijvoorbeeld Ghost. Hierdoor kan in geval van een ramp waarbij zowel je IT omgeving als je unattended-install omgeving in rook zijn opgegaan, een (semi-)unattended install vanaf deze CD of DVD gedaan worden. Een tweede mogelijkheid zou kunnen zijn om LiveCD's te maken met bepaalde services. Bijvoorbeeld servers met SMTP, DNS en authenticatie services. Variabele data zoals de LDAP database of de zone files kunnen op USB stick staan. De LiveCD moet uiteraard wel geconfigureerd zijn om de USB stick te gebruiken voor hun variabele data.

Referenties

[1] **The New Scope of Business Continuity**
Elaine S. Price - www.edocmagazine.com July/August 2004

[2] **Developing a Succesful Network Disaster Recovery Plan**
Bruce Edwards - Information Management & Computer Security, Vol. 2 No. 3, 1994

[3] **Testing the Disaster Recovery Plan**
Bruce Edwards and John Cooper - Information Management & Computer Security, Vol. 3 No. 1, 1995

[4] **Risk & Reliability 5th edition**
Risk & Reliability Associates (R2A) -
www.r2a.com.au/publications/5th_Edition/07_topdown.html