Van ontwijken naar uitwijken

over het uitwijken van de informatievoorziening na een calamiteit

papernote nr 15

Van ontwijken naar uitwijken

Over het uitwijken van de informatievoorziening na een calamiteit

CIP-gegevens Koninklijke Bibliotheek, Den Haag

M.E.M. Spruit | G.A. Ven | W.B.M. Vrouwenvelder | P. Wielaard

Van ontwijken naar uitwijken. Over het uitwijken van de informatievoorziening na een calamiteit.
M.E.M. Spruit | G.A. Ven | W.B.M. Vrouwenvelder | P. Wielaard
Den Haag, Stichting Het Expertise Centrum
ISBN 90-75239-18-1
Trefwoorden: ICT, Informatiebeveiliging, rampenplan, calamiteit, projectmanagement
1e druk november 2003

Vormgeving
Ontwerpbureau Smidswater [bno], Den Haag

Lithografie/druk
Smeink, Amsterdam

Van ontwijken naar uitwijken

Over het uitwijken van de informatievoorziening na een calamiteit

dr. M.E.M. Spruit
ing. G.A. Ven
drs. W.B.M. Vrouwenvelder
ir. P. Wielaard

papernote nr. 15

De volgende papernotes zijn verschenen:

1. *Informatisering: spel zonder grenzen* (1994) – Prof. Dr. E.J.J.M. Kimman
2. *Het recht van overheidsinformatisering* (1995) – Mr. V.A. de Pous
3. *Lichtsporen en luchtspiegelingen* (1996) – Drs. S.B. Luitjens (red.)
4. *Voorbij 2000 ...* (1997) – Drs. S.B. Luitjens, Mw. H. Krijgsman-Heersink en Mr. V.A. de Pous
5. *Oups!* (1998) – Dr. B. Scheepmaker
6. *Digitaal Documentbeheer* (1998) – Dr. J.J.M. Uijlenbroek
7. *Op weg naar E-day; de euro in de overheidsinformatisering* (1998) – drs. J.A. Perlee en drs. M. Rijn
8. *E-commerce; elektronisch zaken doen bij de overheid* (2000) – ir. P.P van der Hijden, drs. A. Jonk, drs. A. W. M. Lasance en dr. J.J.M. Uijlenbroek
9. *Het Resultaat Geteld; over verantwoording en informatievoorziening* (2000) – dr. R. van Dael, drs. W.J. van Gelder en drs. A. Jonk
10. *Overheid in het web; naar een toegankelijke overheidssite* (2001) – Albert G. Arnold, Lucas Swennen, Pieter-Bas Nederkoorn en Reinier Herpel
11. *De politieke partij in de netwerksamenleving* (2002) – Arnold Jonk en Geke van Velzen (red.)
12. *Informatiebeveiliging voor de overheid* (2002) – Boudien Glashouwer, Martin de Graaf, Jeroen Meij, Petra Mettau en Paul Wielaard
13. *De I-functie verklaard* (2002) – Ruud van Dael en Indra Henneman
14. *Aanbesteden van ICT projecten* (2003) – Jacques van Berkel, Auke Bloembergen, Arnold Jonk en Christon Kolk

De volgende notebooks zijn verschenen:

1. *Overheidsinformatisering: het taaie ongerief* (1999) – prof. ir. P.A. Tas en drs. S.B. Luijtjens
2. *Designing electronic document infrastructures* (1997) – dr. J.J.M. Uijlenbroek
3. *Beheerst beheren; beheer van ICT voorzieningen uit managementoptiek* (2000) – ir. H.A. Spanjersberg en mr. dr. ir. Th.J.G. Thiadens

Ten geleide

Informatiebeveiliging is actueel. Met grote regelmaat verschijnen er berichten in de media dat er een bedrijf of instantie is getroffen door een calamiteit. Soms beperkt de calamiteit zich tot één organisatie, andere keren worden er vele getroffen. Sommige calamiteiten halen het nieuws, maar vele ook niet. Calamiteiten komen vaker voor dan u denkt. Elk moment kan er een brand uitbreken, de bliksem inslaan, een grootschalige stroomstoring optreden, of een nieuw computervirus losbarsten. De brand in het Smedinghuis – een kantoorpand van het Ministerie van Verkeer en Waterstaat – was zo'n calamiteit. De foto op de voorkant spreekt voor zich. Als er een calamiteit optreedt, dan weten de hulpdiensten in het algemeen wel raad met schade aan huis en haard. Maar, hoe zit het met schade aan de informatiesystemen en de peperdure gegevens daarin? Organisaties worden steeds afhankelijker van hun informatievoorziening. En dus ook van de computer- en netwerksystemen die daarvoor nodig zijn. Toch zijn de meeste organisaties onvoldoende voorbereid om het hoofd te bieden aan calamiteiten die de informatievoorziening treffen. En dat terwijl met uitwijkvoorzieningen dit soort calamiteiten goed is op te vangen.
Het Ministerie van Verkeer en Waterstaat en Het Expertise Centrum werden via de brand in het Smedinghuis geconfronteerd met zo'n calamiteit die de informatievoorziening trof. Dit was aanleiding om met elkaar deze papernote te schrijven. Het is een handzaam overzicht dat laat zien hoe u zich goed kunt voorbereiden op een eventuele calamiteit en hoe u aansluitend een goede uitwijk voor de informatievoorziening kunt realiseren. Het motto is "van ontwijken naar uitwijken" (oftewel van gewone maatregelen tegen bedreigingen die zich vaak manifesteren, naar uitwijkvoorzieningen voor zelden voorkomende rampen).

Met deze papernote bieden de auteurs u een handvat, waarmee u zelf het nut en de noodzaak van uitwijkmogelijkheden voor uw organisatie kunt inschatten.

Wij wensen u veel leesplezier,

's-Gravenhage, november 2003

Het Expertise Centrum
Drs. L.J.E. Smits
Directeur

Het Ministerie van Verkeer en Waterstaat
Drs. P. Heij
Plaatsvervangend Secretaris Generaal

Inhoudsopgave

Samenvatting

Bedreigingen zoals overstroming, blikseminslag, elektriciteitsstoring, inbraak, fraude, diefstal, hacking, computervirus, etc. kunnen elke organisatie treffen. In uitzonderlijke gevallen leidt zo'n bedreiging tot zeer ernstige schade; er is dan sprake van een calamiteit. Bij een calamiteit worden één of meer primaire bedrijfsprocessen ernstig verstoord.

Hoewel veel organisaties één of meer rampenplannen hebben die beschrijven hoe er gereageerd moet worden op calamiteiten, voorzien deze plannen meestal onvoldoende in reacties op calamiteiten die betrekking hebben op de informatievoorziening. Juist nu steeds meer organisaties steeds afhankelijker worden van hun informatievoorziening is een dergelijke lacune zeer risicovol. Organisaties dienen rekening te houden met calamiteiten die alleen, of met name de informatievoorziening treffen.

Om de continuïteit van de informatievoorziening na een calamiteit zeker te kunnen stellen, kan gebruik gemaakt worden van de maatregel uitwijken, oftewel het terugvallen op een reservefaciliteit als de eigen faciliteit niet meer beschikbaar is. In het Engels wordt *uitwijken* ook wel aangeduid met de term *'disaster recovery'*.

Een uitwijkfaciliteit kan op verschillende plaatsen gerealiseerd worden, namelijk:
- binnen de *eigen organisatie*;
- bij een *soortgelijke organisatie (bilaterale uitwijk)*;
- bij een *gespecialiseerde organisatie*.

Uitwijken is een beveiligingsmaatregel die te beschouwen is als een iteratief proces, dat de volgende stappen doorloopt:
- *risicoanalyse* om de noodzaak van uitwijk te bepalen;
- *selectie* van de soort uitwijk en de uitwijkoplossing;
- *planning* van uitwijk, oftewel het opstellen van het uitwijkplan;
- *implementatie* van het uitwijkplan;
- *onderhoud* van de apparatuur, programmatuur en documentatie;
- *evaluatie* door de directie van de organisatie.

Het kunnen invoeren van uitwijken als beveiligingsmaatregel vereist dat aan een tweetal randvoorwaarden is voldaan, te weten:
- Informatiebeveiliging dient binnen de organisatie *georganiseerd* te zijn.
- Binnen de organisatie dient men zich *bewust* te zijn van het nut van uitwijken.

Als aan deze randvoorwaarden voldaan is, dan dient aan de hand van de uitgevoerde risicoanalyses bepaald te worden welke systemen en voorzieningen voor uitwijken in aanmerking komen. Indien hiervoor een uitwijkvoorziening nodig is, dan wordt een project opgezet dat tot doel heeft de selectie-, planning- en implementatiestap van het uitwijkproces te doorlopen om tot een adequate uitwijkvoorziening te komen. Het op te stellen uitwijkplan en het hierin beschreven uitwijkscenario spelen hierbij een belangrijke rol.

Om uitwijken adequaat in te kunnen richten dient men rekening te houden met de volgende aandachtspunten:
- Net als informatiebeveiliging is uitwijken een zaak van de directie. Het betreft immers het zekerstellen van primaire bedrijfsprocessen na een calamiteit.
- Uitwijken is geen op zichzelf staande maatregel. Het dient dan ook geïntegreerd te worden met andere (beveiligings)processen.
- Communicatie speelt een belangrijke rol in het uitwijkproces. Het betreft hierbij niet alleen de direct betrokkenen binnen en buiten de organisatie, maar ook de andere medewerkers, de klanten en de leveranciers.
- Uitwijken van de informatievoorziening staat of valt met een goed backup-regime. Van alle relevante programmatuur en gegevens dienen contentieus backups gemaakt te worden.
- Zoals elk iteratief proces, dient ook het uitwijkproces continu aandacht te krijgen, om voldoende aan te blijven sluiten op de veranderende organisatie.

Tenslotte kunnen we opmerken dat uitwijken er is voor het opvangen van calamiteiten. Het is te beschouwen als een soort verzekering. Het is dus niet bedoeld voor het opvangen van bedreigingen die regelmatig voorkomen. Daarvoor dienen preventieve maatregelen getroffen te worden. De directie dient ervoor te zorgen dat zowel uitwijken als andere informatiebeveiligingsmaatregelen adequaat uitgevoerd worden.

Hoofdstuk 1

Inleiding

1.1 Casus Rijkswaterstaat

Op zondagmorgen 12 januari 2003 raakt een gebouwencomplex van Rijkswaterstaat in Lelystad door brand fors beschadigd. In dit complex, het Smedinghuis, huizen op dat moment het Rijksinstituut voor Integraal Zoetwaterbeheer en Afvalwaterbehandeling (RIZA) en de Regionale Directie IJsselmeergebied (RDIJ). Het hoofdgebouw met circa 460 werkplekken is door deze brand meerdere jaren onbruikbaar. Overige delen van het complex met circa 360 werkplekken konden 2 tot 4 weken niet worden bewoond. Door de brand, maar meer nog door de rook-, roet- en waterschade, zijn veel bestanden, dossiers en computers onbruikbaar geworden. De serverruimte van RDIJ in het hoofdgebouw ging geheel verloren. Die van RIZA bleef gelukkig gespaard.

Hoewel er geen sprake was van een uitwijkvoorziening voor een dergelijke calamiteit, was er op de dag van de brand al een aanbod van Getronics om een servicedesk en 100 werkplekken met ICT-voorzieningen beschikbaar te stellen. Vanaf dinsdag 14 januari tot 7 februari is van die voorzieningen gebruik gemaakt. Met behulp van de bij Getronics bewaarde back-ups en snel opgezette verbindingen met het netwerk van het Ministerie van Verkeer en Waterstaat konden de belangrijkste ICT-voorzieningen binnen enkele dagen weer beschikbaar gesteld worden. Gezien het beperkte aantal beschikbare werkplekken zijn er veel CD's gebrand, waarmee medewerkers thuis of elders weer aan de slag konden.

Naast de provisorische uitwijkvoorziening is er keihard gewerkt aan het vinden en inrichten van tijdelijke huisvesting in de gebouwen Eurotower (RIZA) en Larserpoort (RDIJ). Ook op ander locaties van Rijkswaterstaat zijn tijdelijk werkplekken gecreëerd. In een race tegen de klok was in gebouw Larserpoort op 10 februari weer een complete serverruimte ingericht met alle daarbij behorende voorzieningen, was er een compleet netwerk aangelegd en waren er ingerichte werkplekken beschikbaar. In de weken daarop is gewerkt aan het structureel herstellen van de benodigde (ICT-)voorzieningen.

Deze ervaring leert dat bij een dergelijke calamiteit veel meer komt kijken dan alleen de ICT regelen. Vooral het vinden van vervangende kantoorruimte en het inrichten daarvan kost veel inspanning. Voor het herstellen van de ICT is het van cruciaal belang dat er goede back-ups beschikbaar zijn, die op een andere locatie bewaard worden dan waar ze gemaakt worden. Het kunnen beschikken over een uitwijkvoorziening helpt enorm om snel weer de meest vitale systemen operationeel te hebben. Het opnieuw inrichten van een complete ICT-omgeving kost nu eenmaal een aantal weken.

.

1.2 Bedreigingen en calamiteiten

Misschien denkt u dat de brand bij Rijkswaterstaat in Lelystad één van die zeldzame gebeurtenissen is waar je nauwelijks rekening mee kunt houden; dat is niet juist. Hoewel grote branden niet heel vaak voorkomen, zijn ze ook niet zeldzaam. Zo werd ongeveer twee maanden eerder, op 20 november 2002, het Rekencentrum van de Universiteit Twente in de as gelegd. Ook daar kostte het heel wat tijd, geld en moeite om de ICT-voorzieningen weer in de lucht te krijgen.

Hoewel brand al vervelend genoeg is, is het slechts één van de vele bedreigingen die een organisatie kunnen treffen. Ook overstroming, blikseminslag, elektriciteitsstoring, inbraak, fraude, diefstal, hacking, computervirus, etc. kunnen een organisatie treffen. Al die verschillende bedreigingen zijn zeer divers van aard. De volgende categorieën van bedreigingen zijn te onderscheiden:

- Menselijke bedreigingen:
  - Onopzettelijk (onoplettendheid, onachtzaamheid, onvoorzichtigheid, etc.).
  - Opzettelijk (diefstal, fraude, sabotage, hacking, computervirus, etc.).
- Niet-menselijke bedreigingen:
  - Externe invloeden (aardbeving, bliksem, wateroverlast, storm, etc.).
  - Storingen in technische voorzieningen (stroomvoorziening, airconditioning, etc.).
  - Storingen in de ICT (apparatuur, programmatuur, gegevens).

Bedreigingen kunnen zelf weer leiden tot een andere bedreiging, die vervolgens in schade resulteert. Zo kan bijvoorbeeld een elektricien onopzettelijk een fout maken, waardoor de elektriciteit wegvalt, hetgeen weer tot storing in een computer leidt. Op deze manier kunnen ketens van bedreigingen ontstaan.

In uitzonderlijke gevallen leidt een bedreiging tot zeer ernstige schade; er

is dan sprake van een calamiteit. Niet elke bedreiging leidt echter tot een calamiteit. We spreken pas over een calamiteit als één of meer primaire processen ernstig verstoord zijn. De verstoring kan betrekking hebben op de locatie (bijvoorbeeld door brand of aardbeving), het personeel (bijvoorbeeld door ernstige besmettelijke ziekte), de financiën (bijvoorbeeld door beursmalaise), of de informatievoorziening (bijvoorbeeld door een nieuw schadelijk computervirus). De brand die het gebouw van Rijkswaterstaat in Lelystad vernielde was een calamiteit met betrekking tot de locatie (verlies van het gebouw) en de informatievoorziening (verlies van het rekencentrum).

Veel organisaties hebben één of meer plannen die beschrijven hoe er gereageerd moet worden op calamiteiten, de zogenaamde rampenplannen. In de rampenplannen staan de taken en verantwoordelijkheden van de interne hulpverleners omschreven, en die van externe partijen, zoals bijvoorbeeld brandweer en politie. Echter, de rampenplannen houden over het algemeen alleen rekening met calamiteiten die betrekking hebben op het personeel en de locatie. Calamiteiten die betrekking hebben op de informatievoorziening worden veelal over het hoofd gezien. Juist nu steeds meer organisaties steeds afhankelijker worden van hun informatievoorziening, dient er ter dege rekening gehouden te worden met calamiteiten die alleen, of met name de informatievoorziening treffen. Hoewel het belang van de informatievoorziening reeds lang onderkend wordt, blijken er slechts weinig organisaties voorbereid te zijn op calamiteiten die hierop betrekking hebben. Deze papernote richt zich met name op de maatregelen die een organisatie dient te treffen om juist dit soort calamiteiten het hoofd te bieden.

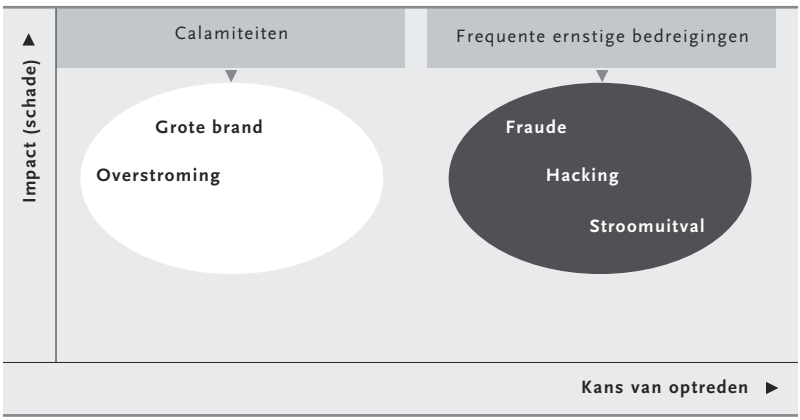
1.3 Beveiligingsmaatregelen

Beveiliging tegen calamiteiten is onder te verdelen in twee soorten maatregelen, te weten:

- *Preventieve maatregelen* die beogen te voorkómen dat een calamiteit überhaupt kan optreden.
- *Repressieve maatregelen* die beogen de schade te beperken als er onverhoopt toch een calamiteit optreedt.

In het kader van “voorkómen is beter dan genezen” is het beter om calamiteiten te voorkómen met preventieve maatregelen. Echter, waterdichte beveiliging is niet mogelijk en zou anders onbetaalbaar zijn. Er is dus behoefte aan een extra vangnet in de vorm van repressieve maatregelen.
In de uitzonderlijke situatie dat er ondanks de preventieve maatregelen toch een calamiteit optreedt, wordt hierdoor de schade beperkt.

Als bedreigingen frequent vóórkomen, dan is de bedrijfsvoering daar in het algemeen op ingesteld. Dit geldt met name voor bedreigingen die ook nog eens aanzienlijke schade op kunnen leveren (het donkere gebied in Figuur 1). Het nut van beveiliging tegen dergelijke bedreigingen is niet omstreden, want het is direct duidelijk welk effect ermee bereikt wordt. Zo zijn er altijd wel (preventieve) maatregelen tegen stroomuitval (UPS), hacking (firewall), fraude (functiescheiding), etc. Anders ligt het bij bedreigingen die zich slechts zelden manifesteren, maar dan wel grote schade opleveren (het lichte gebied in Figuur 1). Dit zijn de bedreigingen waartegen particulieren zich in het algemeen verzekeren. Hierbij valt te denken aan storm, brand, overstroming, ongeval, etc. Ook organisaties kunnen er voor kiezen om zich tegen dergelijke bedreigingen te verzekeren. Maar verzekeren is niet altijd mogelijk of haalbaar. Als verzekeren niet mogelijk of wenselijk is, dan is uitwijken veelal het alternatief.



Figuur 1: Calamiteiten en frequente ernstige bedreigingen

In sommige situaties is het realiseren van calamiteitenvoorzieningen, zoals uitwijk, zelfs (wettelijk) verplicht. Zo zijn bijvoorbeeld gemeenten voor hun Gemeenschappelijke Basisadministratie (GBA) volgens de Wet GBA verplicht om uitwijk te regelen. Het staat gemeenten overigens wel vrij om zelf hiervoor hun eigen invulling te kiezen.

1.4 Informatievoorziening en VBTB

In de Miljoenennota 1999 heeft de regering aangekondigd met voorstellen te komen tot verbetering van de informatiewaarde en de toegankelijkheid

van de departementale begrotings- en verantwoordingsstukken. De nota 'Van beleidsbegroting tot beleidsverantwoording' (VBTB; populair gezegd 'Van Belofte tot Bewijs') bevat deze voorstellen. De kern van VBTB is een samenhang aan te brengen tussen beleidsdoelstellingen, prestaties en middelen, waardoor de begrotings- en verantwoordingsstukken niet alleen een uniforme structuur maar ook een meer beleidsmatig karakter krijgen. De beoogde effecten en bereikte resultaten staan centraal. VBTB is daarmee geen papieren exercitie, maar geeft een structurele impuls aan resultaatgericht management binnen de Rijksdienst. VBTB is tegelijkertijd een omvangrijke en complexe operatie waarbij veel actoren vanuit verschillende invalshoeken zijn betrokken. VBTB doortrekt als het ware alle ministeries en alle processen en heeft op indringende wijze invloed op de manier waarop de ministeries resultaatgericht willen gaan werken.

Eén van de belangrijkste onderdelen van VBTB is de invoering van een bedrijfsvoeringsparagraaf met een 'mededeling bedrijfsvoering'. Onder integrale bedrijfsvoering wordt verstaan: "het geheel van activiteiten voor de aanwending van financiële, personele, materiële en informatiemiddelen voor de beleids- en begrotingsprocessen waarvoor een Minister verantwoordelijkheid draagt"[1]. Met de ontwikkeling van VBTB zal de aandacht voor het financieel beheer derhalve in een breder perspectief worden geplaatst. Niet alleen de financiële administratie, maar ook de sturing en beheersing van de bedrijfsprocessen is object van onderzoek. Door VBTB zullen de uitdagingen waarvoor de ministeries zich gesteld zien op het punt van de bestuurlijke informatievoorziening, toenemen. Het belang en de reikwijdte van het informatievoorzieningsproces zullen namelijk fors uitbreiden. Daarbij gaat het om de rol die informatie gaat spelen, de wijze waarop het proces van informatievoorziening wordt georganiseerd en de vraag hoe besturing en beheersing van het informatieproces zal worden vormgegeven. Aangezien informatiebeveiliging een belangrijk bedrijfsproces is, zullen de ministeries zich moeten beraden op welke wijze zij kunnen verklaren dat zij gedurende het proces 'in control' zijn en welke keuzes zij moeten maken bij de bestuurlijke informatievoorziening. Hierbij is het zaak om afwegingen te kunnen maken over urgentie, schade en prioriteitstelling rondom vraagstukken van informatiebeveiliging.

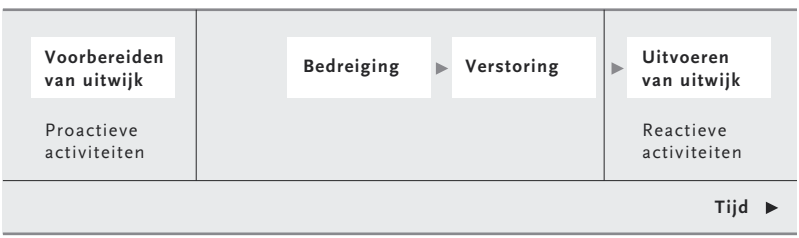
1 *Uit regeringsnota VBTB*

Hoofdstuk 2

Wat is uitwijken

Uitwijken is het terugvallen op een reservefaciliteit, als de eigen faciliteit niet meer beschikbaar is. Veelal wordt de mogelijkheid om uit te wijken gebruikt om de continuïteit zeker te kunnen stellen na het optreden van een calamiteit. In het Engels wordt uitwijken dan ook aangeduid met de term *'disaster recovery'*. Minder gangbare, maar zeer bruikbare, toepassingen voor uitwijken zijn het zekerstellen van de continuïteit bij verhuizing, of bij migratie naar een andere ICT-infrastructuur.

Een uitwijk wordt in het algemeen pas uitgevoerd nadat een calamiteit opgetreden is; het doet niets ter voorkoming van een calamiteit, maar brengt alleen de getroffen informatievoorziening weer in de lucht. Uitwijken is een reactieve activiteit (zie Figuur 2). Een uitwijk kan echter niet zonder meer uitgevoerd worden: er dienen eerst voorbereidende maatregelen getroffen te worden, zoals het kiezen van een uitwijkfaciliteit en het maken van goede afspraken daaromtrent. Deze activiteiten, de zogenaamde proactieve activiteiten, dienen al uitgevoerd te zijn voordat de uitwijkfaciliteit in geval van een calamiteit nodig is.



Figuur 2: Proactieve en reactieve uitwijkactiviteiten

2.1 Soorten uitwijk

Uitwijken heeft veelal betrekking op de technische componenten van de informatievoorziening, zoals de computer- en netwerksystemen. In dit geval worden na een calamiteit alle benodigde technische componenten elders operationeel gemaakt en spreken we van *technische uitwijk*. Het kan echter

ook nodig zijn om niet alleen de technische componenten van de informatievoorziening elders op te bouwen, maar de gehele dienstverlening. In dat geval is er sprake van *functionele uitwijk*, en moet er naast het opbouwen van de technische componenten ook het een en ander geregeld worden voor het verplaatsen van personeel en het inrichten van ruimten en faciliteiten die het personeel nodig heeft, zoals bijvoorbeeld telefoon en administratieve ondersteuning. Als een calamiteit alleen technische componenten treft, zoals een computercentrum, dan is technische uitwijk voldoende.
Als calamiteiten daarentegen een groter deel van de organisatie treffen, dan is functionele uitwijk nodig.

Technische uitwijk wordt mogelijk gemaakt door naast de eigen ICT-infrastructuur nog een reserve ICT-infrastructuur te regelen. Nadat een calamiteit de eigen infrastructuur treft, worden alle belangrijke informatiesystemen op de reserve infrastructuur operationeel gemaakt.
Voor functionele uitwijk dienen daar dan nog andere faciliteiten aan toegevoegd te worden, zoals gemeubileerde werk- en vergaderruimten, telefoonvoorziening, etc.

De technische uitwijkfaciliteit (de reserve ICT-infrastructuur) kan op verschillende plaatsen gerealiseerd worden, namelijk:

- Binnen de *eigen organisatie*. Indien de eigen organisatie voldoende ruim in de ICT-middelen zit, dan kan een deel daarvan aangemerkt worden als reserve. Dit kunnen middelen zijn die normaal gesproken gebruikt worden voor weinig urgente zaken, zoals bijvoorbeeld ontwerpen of testen. Indien belangrijke ICT-middelen door een calamiteit getroffen worden, dan worden de daarop draaiende informatiesystemen overgezet op de reservemiddelen. Eventuele daarop draaiende niet-urgente systemen worden tijdelijk uitgeschakeld.
- Bij een *soortgelijke organisatie (bilaterale uitwijk)*. Organisaties die een vergelijkbare informatievoorziening hebben kunnen onderling afspreken dat ze in het geval van een calamiteit de eigen ICT-infrastructuur voor de ander beschikbaar stellen. Aangezien in dat geval twee organisaties gebruik maken van één ICT-infrastructuur, kunnen beide gedurende de uitwijkperiode slechts de belangrijkste informatiesystemen draaien.
- Bij een *gespecialiseerde organisatie*. Indien men ervoor kiest om de uitwijkfaciliteit te regelen bij een daarin gespecialiseerde organisatie dan krijgt men niet alleen de beschikking over de benodigde infrastructuur, maar ook de bijbehorende deskundigheid. De gespecialiseerde organisatie kan bijvoorbeeld ondersteuning leveren bij het veiligstellen van backups, het opstellen van een uitwijkplan en het trainen van personeel.

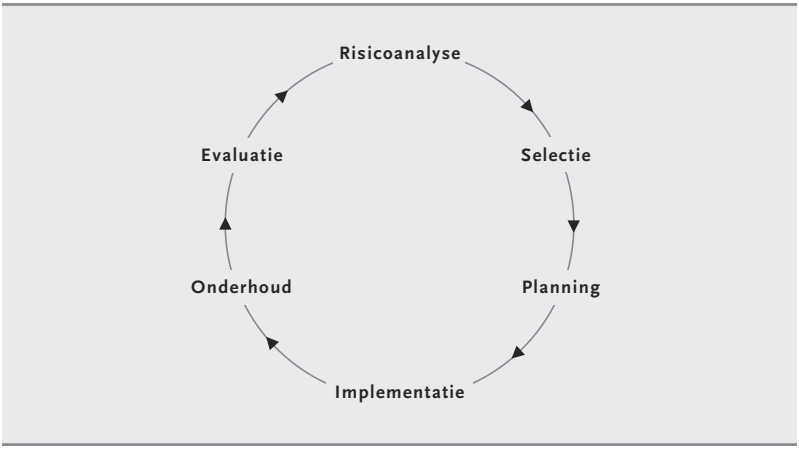
2.2 Technische uitwijkoplossingen

In het geval van een technische uitwijk dient een uitwijkfaciliteit binnen een van tevoren bepaalde tijd beschikbaar te zijn voor de informatiesystemen die moeten uitwijken. Afhankelijk van de eisen die op dit punt gesteld worden zijn er verschillende soorten uitwijkfaciliteiten:

- Een *container* met een beperkte ICT-infrastructuur (computer- en netwerksystemen), die voldoende is om alle uit te wijken informatiesystemen op te draaien. In het geval van een calamiteit kan de container binnen korte tijd naar de plek des onheils getransporteerd worden. Daar hoeft deze alleen nog aangesloten te worden op de elektriciteit en zonodig op het nog beschikbare netwerk. Vervolgens worden de benodigde programmatuur en gegevens geïnstalleerd en gestart. De tijd die gemoeid is met het brengen van de container en het operationaliseren van de informatiesystemen varieert van enkele uren tot meer dan een dag. Deze uitwijkmogelijkheid is relatief goedkoop.
- Een *'empty shell'*, oftewel een lege ruimte die voorbereid is om de benodigde ICT-infrastructuur in onder te brengen. Dit betekent dat de basisvoorzieningen zoals bijvoorbeeld elektriciteit wel aanwezig zijn, maar de ICT-infrastructuur zelf nog niet. Pas als uitwijken nodig is, worden de benodigde computer- en netwerksystemen van elders aangevoerd en geïnstalleerd. Vervolgens worden programmatuur en gegevens geïnstalleerd en gestart. De tijd die gemoeid is met het aanvoeren en installeren van de apparatuur en het operationaliseren van de informatiesystemen varieert van enkele uren tot meer dan een dag. Deze uitwijkmogelijkheid is meestal duurder dan de uitgeruste container, behalve als er ruimte in overvloed is. De ICT-infrastructuur is echter beter te beveiligen.
- Een *'cold' redundant faciliteit*, oftewel een volledige ICT-infrastructuur, inclusief alle benodigde programmatuur en gegevens, die beschikbaar is om ingezet te worden. Als uitwijken nodig is, dan wordt alles opgestart, waarna de gegevens vanaf backup geactualiseerd worden. De tijd die hiermee gemoeid is, ligt in de orde van enkele uren. Deze uitwijkmogelijkheid is beduidend duurder dan de 'empty shell'. Zolang de ICT-infrastructuur niet nodig is voor uitwijken kan deze echter ingezet worden voor andere doeleinden, zoals bijvoorbeeld ontwerp- en testactiviteiten.
- Een *'hot' redundant faciliteit*, oftewel een volledig operationele dubbel uitgevoerde informatievoorziening. Alle informatiesystemen die anders uit zouden moeten kunnen wijken, draaien in tweevoud op verschillende ICT-infrastructuren ('mirroring'). Als op één van de twee infrastructuren een informatiesysteem problemen ondervindt, dan wordt automatisch overgeschakeld naar het identieke systeem op de andere infrastructuur.

Er is weinig of geen tijd gemoeid met het terugvallen op de 'mirror'. Daar staat tegenover dat deze uitwijkmogelijkheid verreweg het duurst is.

2.3 Het uitwijkproces



Figuur 3: Het uitwijkproces

Uitwijken is een beveiligingsmaatregel die te beschouwen is als een iteratief proces. Het proces doorloopt de volgende stappen (zie Figuur 3):

- Risicoanalyse om de noodzaak van uitwijk te bepalen. Uit risicoanalyse volgt welke informatiesystemen (en daarvoor benodigde middelen) zodanig belangrijk zijn voor de organisatie dat ze in aanmerking komen voor uitwijk. Bovendien kan aan de hand van risicoanalyse bepaald worden hoeveel de uitwijkvoorziening mag kosten.
- Selectie van de soort uitwijk (eigen, soortgelijke, of gespecialiseerde organisatie) en de uitwijkoplossing (container, empty shell, cold redundant, of hot redundant) die de organisatie prefereert. In deze fase wordt veelal ook gekozen bij welke partij de uitwijkfaciliteit geregeld gaat worden.
- Planning van uitwijk, oftewel het opstellen van het uitwijkplan. Het uitwijkplan bevat enerzijds een beschrijving van de proactieve uitwijkactiviteiten, zoals de backup-procedures, en anderzijds het uitwijkscenario waarin alle reactieve uitwijkactiviteiten beschreven staan, alsmede de organisatie van uitwijk.
- Implementatie van het uitwijkplan. In deze stap worden de contracten met externe partijen afgesloten. Voor zover nieuwe middelen nodig zijn

worden deze gerealiseerd. De bij uitwijk betrokken mensen krijgen zonodig opleiding en training en de benodigde procedures worden ingevoerd.
- Onderhoud van de apparatuur, programmatuur en documentatie van de uitwijkfaciliteit, alsmede de zorg dat de faciliteit meegroeit met veranderingen in de primaire ICT-infrastructuur. In deze fase worden op gezette tijden backups gemaakt en getest. Tevens wordt het uitwijkscenario regelmatig geoefend om zeker te stellen dat de inhoud ervan klopt en voldoende bekend is bij alle betrokkenen.
- Evaluatie door de directie van de organisatie om te bepalen of de gerealiseerde invulling van uitwijk voldoende tegemoet komt aan de behoeften van de organisatie.

Hoofdstuk 3

De implementatie

Het kunnen invoeren van uitwijken als beveiligingsmaatregel vereist dat aan een tweetal randvoorwaarden is voldaan, te weten:

- Informatiebeveiliging dient *georganiseerd* te zijn. Uitwijken is een informatiebeveiligingsmaatregel die binnen het verantwoordelijkheidsdomein van informatiebeveiliging geregeld moet worden. Dit houdt onder meer in dat de verantwoordelijkheden ten aanzien van informatiebeveiliging in de organisatie goed belegd zijn en dat het management van de organisatie informatiebeveiliging voldoende prioriteit geeft.
- Binnen de organisatie dient men zich *bewust* te zijn van het nut van de maatregel uitwijken. In het algemeen betekent dit dat er enige stappen van bewustwording ten aanzien van informatiebeveiliging doorlopen zijn, of dat het bewustzijn stantepede is gecreëerd door een opgetreden calamiteit. Het nut en de reikwijdte van uitwijken kunnen overigens bepaald worden met behulp van risicoanalyse.

Als aan deze randvoorwaarden voldaan is, dan dient aan de hand van de uitgevoerde risicoanalyses bepaald te worden welke systemen en voorzieningen voor uitwijken in aanmerking komen. Indien hiervoor een uitwijkvoorziening nodig is, dan wordt een project opgezet dat tot doel heeft de selectie-, planning- en implementatiestap van het uitwijkproces te doorlopen om tot een adequate uitwijkvoorziening te komen. Het op te stellen uitwijkplan en het hierin beschreven uitwijkscenario spelen hierbij een belangrijke rol.

3.1 Het uitwijkplan

In het uitwijkplan, ook wel 'calamiteitenplan voor de informatievoorziening' genoemd, staat wat er geregeld dient te worden om uitwijk te kunnen realiseren. Het plan beschrijft onder meer:

- De organisatie van uitwijken en de relaties met het management en eventuele externe partijen.
- De uitwijkfaciliteit, alsmede de contractuele afspraken die daarover gemaakt zijn.

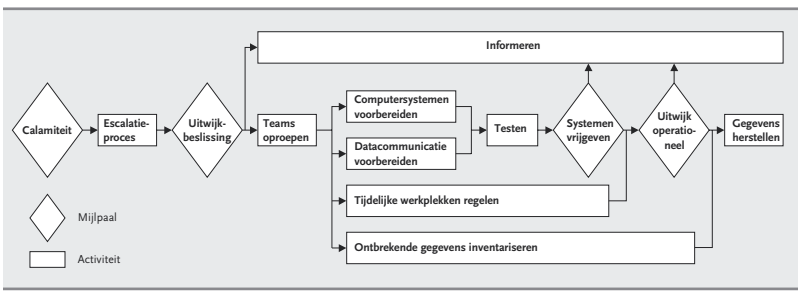
- De informatiesystemen en de ICT-middelen die in aanmerking komen om uit te wijken.
- De procedures voor het maken, toetsen, opslaan en vernietigen van backups.
- De procedures voor het uitvoeren van uitwijktesten en het actualiseren van de uitwijkconfiguratie en -documentatie.
- Het uitwijkscenario, waarin beschreven wordt welke activiteiten uitgevoerd worden in het geval van een uitwijk.

Het uitwijkplan staat niet los van andere calamiteitenplannen. De directie dient ervoor te zorgen dat een uitwijkvoorziening voor de informatievoorziening afgestemd is op de andere zaken die voor calamiteiten worden geregeld. In het uitwijkplan worden de relaties met de andere calamiteitenvoorzieningen beschreven.

3.2 Het uitwijkscenario

Het uitwijkscenario beschrijft de activiteiten die uitgevoerd worden in het geval van een uitwijk. Bovendien geeft het aan welke teams en functionarissen betrokken zijn bij het uitwijken en hoe de verantwoordelijkheden en bevoegdheden verdeeld zijn. Het uitwijkscenario beschrijft de volgende elementen:

- Het escalatieproces, dat is het proces dat leidt tot de beslissing of er al dan niet uitgeweken gaat worden.
- De mijlpalen en activiteiten voor het uitvoeren van een uitwijk (zie Figuur 4).
- De teams en functionarissen en hun verantwoordelijkheden en bevoegdheden.



Figuur 4: Een vereenvoudigde schets van een uitwijkscenario

Hoofdstuk 4

Best practice

Uit de ervaring van vele organisaties die slachtoffer waren van een calamiteit, en hun uitwijk al dan niet goed geregeld hadden, kan men veel informatie putten. Enkele belangrijke aandachtspunten worden hieronder weergegeven, onderverdeeld naar punten die spelen vóór respectievelijk na de uitwijk.

4.1 Voordat er uitgeweken moet worden

In principe wordt het hele uitwijkproces zoals dat eerder beschreven is, uitgevoerd voordat er uitgeweken kan worden. Dit betekent onder meer dat risicoanalyses uitgevoerd zijn om te bepalen welke informatiesystemen uit moet kunnen wijken en dat de resultaten daarvan input zijn voor het opstellen van een uitwijkplan. Enkele aspecten die wellicht onderschat of zelfs over het hoofd gezien worden, worden hieronder beschreven.

Aandacht van de directie

Uitwijken is geen maatregel ten behoeve van beveiligingsmedewerkers, maar is het zeker stellen van cruciale middelen voor bedrijfsprocessen. De directie trekt deze kar. Zij bepaalt hoe lang bepaalde bedrijfsprocessen uit mogen vallen en welke informatiesystemen door uitwijken weer snel in de lucht moeten komen. De directie draagt ook de kosten voor de uitwijkvoorziening en stelt daar zonodig grenzen aan.

Risicoanalyses combineren

In het kader van informatiebeveiliging worden al risicoanalyses uitgevoerd. Het heeft geen zin om deze analyses nog eens dunnetjes over te doen als onderdeel van het uitwijkproces. Het is zaak om alle relevante aspecten voor het uitwijken te betrekken bij de risicoanalyses die al voor informatiebeveiliging uitgevoerd worden.

Datacommunicatiefaciliteiten

Bij het bepalen van de informatiesystemen die moeten kunnen uitwijken, worden de datacommunicatiefaciliteiten nogal eens over het hoofd gezien. Veel informatiesystemen zijn zonder datacommunicatie echter niet goed

inzetbaar. In die gevallen moeten geschikte datacommunicatiefaciliteiten deel uitmaken van de uitwijkfaciliteit.

Informeren van betrokkenen
Degenen die het meest direct de consequenties van een calamiteit ervaren zijn de eigen medewerkers van de organisatie. Zij dienen goed op de hoogte gehouden te worden, zowel over de calamiteit als over de follow-up.
Bij rampen die lichamelijke of psychische impact hebben is het bovendien nodig om de medewerkers goed op te vangen. De afdeling communicatie of personeelszaken kan hierbij een belangrijke rol spelen.

Naast de medewerkers zijn ook de afnemers en de toeleveranciers direct betrokken bij de calamiteit. Zij ervaren de calamiteit doordat de productie stokt en wellicht voorraden verloren gegaan zijn. Bovendien kunnen administratieve processen haperen. Ook afnemers en toeleveranciers zijn gebaat bij goede en tijdige informatieverschaffing. Veelal wordt het op prijs gesteld als men rechtstreeks geïnformeerd wordt en het niet eerst in de krant moet lezen.

Informeren van derden
Bij calamiteiten zijn externe partijen betrokken, zoals politie, brandweer, gemeente, etc. Van tevoren dient nagedacht te zijn welke instanties na een eventuele calamiteit op de hoogte gebracht moeten worden en welke informatie ze nodig hebben.

Bovendien is een ramp die zich voltrekt moeilijk uit het nieuws te houden. Om het imago geen al te grote deuk op te laten lopen, is het verstandig om zelf de regie te voeren bij het verschaffen van informatie aan de media. Van tevoren dient nagedacht te worden welke media geïnformeerd moeten worden en wie daarvoor de woordvoerder respectievelijk penvoerder moet zijn.

Maken en opslaan van backups
Als er uitgeweken moet worden dan zijn backups nodig van alle relevante programmatuur en gegevens. Deze backups moeten dan wel actueel en compleet zijn. Een goed backup-regime is dan ook een noodzakelijke randvoorwaarde voor uitwijken, evenals een strikte naleving van het backup-regime. Bovendien dienen backups op een veilige locatie opgeslagen te worden. Opslag van backups in de nabijheid van computersystemen mag dan handig zijn, het is in het geval van een calamiteit in het algemeen geen veilige plaats.

Continue aandacht voor uitwijkvoorziening
Het hele conglomeraat van apparatuur en daarop draaiende applicaties binnen een organisatie zal regelmatig wijzigen. Deze wijzigingen kunnen impact hebben op de gerealiseerde uitwijkvoorziening. Men dient hierop bedacht te zijn en uitwijken continu aandacht te geven. Ook het regelmatig uitvoeren van uitwijktesten vervult hierbij een nuttige rol.

4.2 Nadat er uitgeweken is

Nadat er uitgeweken is naar een uitwijkfaciliteit, is het belangrijkste deel van de informatievoorziening weer operationeel. Er dient dan wel snel een aanvang te worden gemaakt met het herstellen van de oorspronkelijke voorzieningen.

Eerste opvang
In de hectische omstandigheden direct na een calamiteit werkt een beperkte groep medewerkers en hulpverleners intensief en in moeilijke omstandigheden aan het opruimen en herstellen van de schade. Deze mensen hebben daarvoor voldoende voorzieningen nodig, zoals noodhuisvesting, verlichting, opslag- en transportmiddelen, gereedschap, eten en drinken, etc.

Telefonische bereikbaarheid
Gedurende de eerste uren na een calamiteit moet er veel gecommuniceerd worden met hulpverleners, personeel en derden. Het is zaak om direct al over een telefoonvoorziening te beschikken. Medewerkers die oproepbaar zijn moeten hun mobiele telefoon aan hebben staan en hun telefoonlijst bij zich hebben.

Personeel informeren
Veel acties naar aanleiding van een calamiteit moeten worden uitgevoerd door en met het personeel. Het is dan zeer ongewenst als juist het personeel niet goed op de hoogte is van de situatie. Zo snel mogelijk een personeelsbijeenkomst organiseren is nodig. Bovendien bevordert zo'n bijeenkomst de teamgeest en daarmee de inzet van het personeel.

Huisvesting
Veel calamiteiten treffen niet alleen de informatievoorziening maar de gehele huisvesting. Aangezien veel uitwijkvoorzieningen slechts beperkte tijd beschikbaar zijn, is er niet al te veel tijd beschikbaar voor het herstellen van de oorspronkelijke huisvesting respectievelijk het realiseren van vervangende huisvesting. Men dient daarom zo snel mogelijk na de calamiteit een begin te maken met het herstel respectievelijk het zoeken en inrichten van

een (al dan niet tijdelijke) vervangende locatie.

Herstel elektronische gegevens
In principe moeten alle belangrijke elektronische gegevens op backup veilig gesteld zijn. Toch komt het voor dat er na een calamiteit blijkt dat er belangrijke gegevens opgeslagen waren op een medium waarvan geen backup gemaakt werd. De gegevens zijn dan bijvoorbeeld te vinden op een door rook zwart geblakerde of door de hitte gebarsten harde schijf. Er zijn gespecialiseerde bedrijven die in staat zijn om zelfs van zo'n schijf nog gegevens te redden, maar ook dat kent grenzen. Bovendien kost het veel tijd en geld.

Papieren informatie
Alleen elektronische gegevens worden met backups veilig gesteld. Na een calamiteit worden de getroffen elektronische gegevens vanaf backup hersteld. De papieren gegevensdragers, zoals documenten, lijsten en kaartenbakken zijn daarmee nog niet hersteld. De gegevens daaruit moeten zo goed mogelijk op een andere wijze gered zien te worden.

Hoofdstuk 5

Tenslotte

Uitwijken is er voor het opvangen van calamiteiten. Het is te beschouwen als een soort verzekering. Het is dus niet bedoeld voor het opvangen van bedreigingen die regelmatig voorkomen. Daarvoor dienen preventieve maatregelen getroffen te worden. De directie dient ervoor te zorgen dat zowel uitwijken als andere informatiebeveiligingsmaatregelen adequaat uitgevoerd worden.

Vanwege de grote schade die met calamiteiten gepaard gaat, is uitwijken voor veel organisaties een noodzakelijke beveiligingsmaatregel. Het zorgt ervoor dat de schade na een calamiteit beperkt blijft. Het realiseren van een geschikte uitwijkvoorziening heeft echter nogal wat voeten in de aarde en kan kostbaar zijn, met name als de ICT-infrastructuur en de applicatieportfolio omvangrijk en heterogeen zijn.

Als een uitwijkvoorziening beschikbaar is dan kan deze eventueel ook ingezet worden voor andere gebeurtenissen die weinig voorkomen maar een grote impact op de organisatie hebben, zoals verhuizing, of migratie naar een andere ICT-infrastructuur. De uitwijkvoorziening kan dan gebruikt worden voor het zekerstellen van de continuïteit van de informatievoorziening.

Literatuur

- CCTA, Contingency Planning, ITIL-reeks, CCTA, Londen, 1994, ISBN 0-11-330524-9.
- B. Glashouwer, M. de Graaf, J. Meij, P. Mettau en P. Wielaard, Informatiebeveiliging voor de overheid, Het Expertise Centrum, Den Haag, 2002.
- R. Hoeffnagel, Wat mag uitwijk kosten?, IT beheer, nr. 2, 2003, blz. 20-24.
- W. Huurman, De noodzaak van continuïteitsmanagement, Informatie, mei, 2003, blz. 40-44.
- J. Jordan, H. Zellenrath & R. Verzuu, Guide to business continuity planning, CSCI/CPA, Weesp, 2002.
- P. Overbeek, E. Roos Lindgreen & M. Spruit, Informatiebeveiliging onder controle, Pearson Education, Amsterdam, 2000, ISBN 90-430-0289-5.
- M. Verheijen & M. Spruit, Use of expert systems to develop disaster recovery scenarios, Contingency Planning & Recovery Journal, vol. 14, nr. 1, 2000, blz. 2-15.

HET EXPERTISE CENTRUM

Een vastgelopen project, een mislukte definitiestudie, een uit de hand gelopen budget ... Kunnen dit soort problemen voorkomen worden? En zo ja, hoe? Complexe vraagstukken. Enkele van de vele. Want het wordt steeds ingewikkelder om de organisatie van de informatievoorziening goed te regelen. Daarom zijn experts gewenst. Deze experts werken bij Het Expertise Centrum. Het Expertise Centrum is een onafhankelijk adviesbureau dat zich bezighoudt met overheidsinformatisering. Het bureau kenmerkt zich door onafhankelijkheid bij het aannemen en uitvoeren van opdrachten. Dat waarborgen wij door de stichtingsvorm. Maar ook door alleen rechtstreeks voor de opdrachtgever te werken en niet als onderaannemer.

Onze consultants kennen de overheidscultuur van zeer dichtbij. Niet alleen van het Rijk, maar ook van de provincies, gemeenten, waterschappen en verzelfstandigde organisaties. Ze hebben daardoor als geen ander inzicht in de bestuurlijke en organisatorische aspecten van de informatievoorziening. En ze kunnen u bijstaan bij problemen van vandaag en het voorkomen van problemen van morgen.

Wat kunnen wij voor u doen?
- Strategische advisering
- Contra-expertise
- Programma- en procesmanagement
- Projectadvisering
- Innovatief onderzoek
- Opleiding en traineeprogramma's

Voor meer informatie kunt u contact opnemen met:
Directeur drs. L.J.E. Smits

STICHTING HET EXPERTISE CENTRUM
Van de Spiegelstraat 12
Postbus 18607
2502 EP Den Haag
telefoon: 070 351 49 97
fax: 070 351 5282
e-mail: info@hec.nl
[www.hec.nl]