Ministerie van Veiligheid en Justitie

Hulpmiddel voor zelfanalyse en vervolgactie

Waarborgen en aandachtspunten voor de continuïteit van uw organisatie

Inleiding

Dit hulpmiddel stelt u in staat om de continuïteit van uw organisatie te bevorderen en haar vitale maatschappelijke functie onder moeilijke omstandigheden te helpen garanderen. In het bijzonder helpen de waarborgen en bijbehorende aandachts-punten in dit document de continuïteit van uw organisatie onder omstandigheden van ICT- of elektriciteitsuitval te bevorderen. Specifiek helpen de waarborgen en aandachtspunten uw organisatie om:

- Uitval te voorkomen
- De voorbereiding op eventuele uitval te verbeteren
- Een uitval en effecten van deze snel en adequaat te kunnen beheersen
- Een snel herstel van de uitval te bevorderen

In dit document presenteren wij tien waarborgen. Deze vormen gezamenlijk een gewenste uitgangssituatie voor het zo goed mogelijk kunnen continueren van uw dienstverlening als de ICT of elektriciteit uitvalt.

De tien waarborgen zijn:

- Waarborg 1: randvoorwaarden voor continuïteitsmanagement
- Waarborg 2: continuïteit vitale maatschappelijke diensten
- Waarborg 3: continuïteit ICT- & informatiebeveiliging
- Waarborg 4: continuïteit elektriciteitsvoorziening
- Waarborg 5: continuïteit crisismanagement
- Waarborg 6: continuïteit communicatie
- Waarborg 7: continuïteit informatievoorziening
- Waarborg 8: continuïteit werkzaamheden en werkomstandigheden
- Waarborg 9: continuïteit dienstverlening derden
- Waarborg 10: continuïteit financiële positie, betalingsverkeer & herstelkosten

Elke waarborg belicht een kernthema en is voorzien van specifieke aandachts-punten. Deze punten zijn bedoeld om uw aandacht te richten op specifieke aspecten van uitval: van het voorkomen en het voorbereiden tot het adequaat reageren en zo snel mogelijk herstellen. De aandachtspunten kunt u gebruiken voor zelfanalyse en -onderzoek. De logica achter de waarborgen en aandachtspunten is als volgt: naarmate uw organisatie meer aandachtspunten heeft ‘behandeld’ en – waar nodig – doorgevoerd, des te beter zal uw organisatie zijn voorbereid op en bestand zijn tegen uitval. De waarborgen zijn allemaal belangrijk maar in principe weergegeven in volgorde van prioriteit. Dit stelt u in staat om al naar gelang de behoefte en mogelijkheden van uw organisatie uit waarborgen te kiezen. Binnen een waarborg kunt u zelf prioriteren door te kiezen welke aandachtspunten voor uw organisatie het meest belangrijk worden gevonden, urgent zijn, het grootste effect sorteren et cetera.

De waarborgen en aandachtspunten zijn gebaseerd op principes van continuïteits-management, onderzoek naar lessen uit recente nationale en internationale cases van ICT- en elektriciteitsuitval en praktijkervaringen van professionals. De waar-borgen en aandachtspunten zijn generiek van aard. Dit houdt in dat zij relevant zijn voor iedere organisatie die geconfronteerd wordt met de gevolgen van ICT- of elektriciteitsuitval. Het kader vervult een functie voor zowel organisaties die mogelijk al verder gevorderd zijn met continuïteitsmanagement, als wel voor organisaties die met continuïteitsmanagement willen starten.

Daarbij past ook direct een belangrijke kanttekening bij dit hulpmiddel: de informatie in dit document biedt weliswaar richting maar behoeft altijd een vertaalslag naar uw eigen organisatie. Alleen u en uw collega's zijn in staat om voor uw organisatie het vereiste maatwerk te leveren. U kent uw organisatie, haar taken, haar risico's en andere relevante kenmerken en bijzonderheden immers het beste. En u en uw collega's zullen uiteindelijk als het er echt op aankomt gezamenlijk de continuïteit van uw organisatie moeten garanderen.

Als relevante achtergrondinformatie bij dit document is, in opdracht van het Ministerie van Veiligheid & Justitie, naast een brochure en bewustmakingsfilm een handleiding ontwikkeld: 'Voorbereid op uitval van elektriciteit en ICT: continuïteitsmanagement voor organisaties met een vitale maatschappelijke functie'. Tevens zijn ten behoeve van zes overheiddoelgroepen specifieke hulpmiddelen voor zelfanalyse en vervolgactie ontwikkeld. Het betreft hier de volgende doelgroepen: rijksoverheden, provincies, waterschappen, veiligheidsregio's, politieregio's en gemeenten. De bewustmakingsfilm, brochure, handleiding en de verschillende hulpmiddelen zijn toegankelijk via www.nationale-veiligheid.nl.

Den Haag, 2010

Waarborg 1: randvoorwaarden voor continuïteitsmanagement

Uw organisatie is zich op alle niveaus bewust van het belang van continuïteitsmanagement. Uw organisatie heeft aan continuïteitsmanagement ontleende principes aantoonbaar ingebed. Als onderdeel van haar continuïteitsmanagement heeft uw organisatie bovendien specifiek aandacht voor de continuïteitsrisico's ICT- en elektriciteitsuitval

Bestuurlijke aandacht garanderen

- Beschouw continuïteitsmanagement als een belangrijke randvoorwaarde voor het zo ongestoord mogelijk laten functioneren van uw organisatie en vitale maatschappelijke dienstverlening
- Bezie continuïteitsmanagement als een uiting van het nemen van maatschappelijke verantwoordelijkheid en van het willen leveren van optimaal betrouwbare en kwalitatief hoogstaande (maatschappelijke) diensten
- Beleg de eindverantwoordelijkheid voor continuïteitsmanagement expliciet bij het bestuur danwel topmanagement

Kwetsbaarheden identificeren

- Analyseer uitgaande van de kerntaken en –belangen van uw organisatie welke activiteiten (processen, diensten, producten et cetera) essentieel zijn voor het continueren van deze kerntaken en -belangen (organisatieanalyse)
- Bepaal de impact van specifieke continuïteitsrisico's op de essentiële activiteiten (impactanalyse). Besteed hierbij in ieder geval aandacht aan de uitval van ICT en elektriciteit. Houd bovendien rekening met risico's als gevolg van bewust menselijk handelen
- Houd de afhankelijkheden van uw organisatie met cruciale derden hierbij duidelijk voor ogen
- Maak gebruik van relevante eerdere inspanningen die uw organisatie, bijvoorbeeld in het kader van de voorbereiding op de H1N1-grieppandemie, heeft geleverd. Benut de mogelijk toen al in kaart gebrachte kritieke processen

Strategie bepalen

- Formuleer op basis van de voornoemde analyses een continuïteitsstrategie.[1] Deze maakt duidelijk welke essentiële activiteiten uw organisatie vervult en aan welke activiteiten uw organisatie de hoogste prioriteit toekent. Daarnaast maakt de strategie inzichtelijk wat ondernomen moet worden om de continuïteit van de essentiële activiteiten te kunnen waarborgen
- Ontleen aan deze strategie een door het bestuur danwel topmanagement vast te stellen beleidsverklaring
- Besteed bij nieuw- of verbouw van ICT, gebouwen en processen specifiek aandacht aan continuïteit
- Maak afspraken voor het herzien en actualiseren van de continuïteitsstrategie

Continuïteit organiseren

- Formuleer op het niveau van het bestuur danwel topmanagement een duidelijke opdracht waarmee het continuïteitsmanagement door uw organisatie van invulling en richting wordt voorzien

[1] Maak hiervoor gebruik van het 'model continuïteitsstrategie' in de Handleiding continuïteitsmanagement

- Wijs een (gedelegeerd) eindverantwoordelijke aan die (gedeeltelijk) is vrijgemaakt en tevens aanspreekbaar is op het continuïteitsmanagement van uw organisatie. Voorzie deze functionaris van een heldere opdracht en een duidelijk mandaat
- Benader continuïteitsmanagement als een programma of op zijn minst een project
- Formuleer een programma- of projectplan om de gestelde continuïteitsstrategie te kunnen behalen
- Zie toe op een (representatieve) organisatiebrede betrokkenheid bij de totstandkoming en uitwerking van continuïteitsmanagement
- Overweeg om het continuïteitsmanagement van uw organisatie vorm te geven conform één van de beschikbare kwaliteitsstandaarden voor continuity management (zie verder de handleiding)
- Voer een periodieke audit uit op de continuïteitsorganisatie en/of integreer de strategie, plannen en activiteiten in de 'planning- & control-' of beheerscyclus van uw organisatie

Continuïteit inbedden

- Maak de organisatie meer bewust van de mogelijke impact van continuïteitsrisico's. Benadruk daarbij de organisatiebrede consequenties van ICT- of elektriciteitsuitval
- Voorzie in ieder geval in drie (deel)plannen. Eén gericht op het beperken van de acute gevolgen van een uitval (deelplan 1: crisismanagement). Een ander bedoeld om de essentiële activiteiten te continueren (deelplan 2: continuïteitsmanagement). En één om een zo snel mogelijk herstel en normalisatie te bevorderen (deelplan 3: herstel)
- Koppel het continuïteitsmanagement nadrukkelijk aan het crisis- en calamiteitenmanagement van uw organisatie. Maak daarbij gebruik van de beschikbare alarmerings- en opschalingsstructuur in uw organisatie
- Test de getroffen voorzieningen onder meer met behulp van gericht trainen en oefenen

Waarborg 2: continuïteit vitale maatschappelijke diensten

Uw organisatie heeft structureel aandacht voor de continuïteit van de door haar geleverde vitale maatschappelijke diensten. Er bestaat aantoonbaar goed zicht op de essentiële activiteiten die de dienstverlening mogelijk maken, als ook de kwetsbaarheden hiervan onder invloed van ICT- of elektriciteitsuitval. Er zijn maatregelen getroffen die de continuïteit van de vitale maatschappelijke diensten helpen waarborgen

Kwetsbaarheden identificeren

- Weet welke van de door uw organisatie uitgevoerde activiteiten het meest essentieel ('vitaal') zijn voor de samenleving
- Onderzoek welke gevolgen ICT- en elektriciteitsuitval hebben voor de beschikbaarheid en leveringszekerheid van uw vitale maatschappelijke dienstverlening
- Bepaal voor uw vitale maatschappelijke dienstverlening de maximaal acceptabele uitvalsperiode c.q. de maximaal acceptabele hersteltijd

Maatregelen treffen

- Zie er door middel van maatregelen op toe dat uw organisatie onder omstandigheden van uitval in staat is om haar dienstverlening zo goed en lang mogelijk te continueren

Waarborg 3: continuïteit ICT- & informatiebeveiliging

Uw organisatie is in staat om de continuïteit van de ICT aantoonbaar zoveel mogelijk te waarborgen. Dat geldt zowel voor de essentiële activiteiten ten behoeve van de samenleving (‘vitale diensten’) als ook voor andere essentiële activiteiten

Kwetsbaarheden identificeren
- Weet van welke systemen de grootste afhankelijkheid bestaat ten behoeve van de continuïteit van essentiële activiteiten
- Onderzoek of en in hoeverre uw organisatie in staat is om zelf de oorzaak van mogelijke uitval te achterhalen (‘diagnostiek’). Tref indien de mogelijkheden hiertoe beperkt zijn, voorzieningen om de diagnostiek – gegarandeerd – door externen te laten plaatsvinden
  - Bepaal of verlies van data acceptabel is en wat het eventuele maximale dataverlies is
  - Besteed expliciet aandacht aan het in kaart brengen van uw cruciale belangen en kwetsbaarheden in het licht van spionage. Maak hiervoor gebruik van de ‘Handleiding Kwetsbaarheidsanalyse Spionage’[2]

Weerbaarheid inventariseren
- Uw organisatie werkt in toenemende mate informatiegedreven. Dit verlangt dat belangrijke operationele en/of sturingsinformatie voorhanden blijft. Bedenk hoe de techniek zo kan worden ingericht en benut dat dit mogelijk wordt

Continuïteit organiseren
- Voer een meldingsplicht in voor ICT-incidenten en zie er op toe dat zwaardere incidenten altijd met tussenkomst van/namens het bestuur worden afgehandeld. Dit om op organisatieniveau de beste afweging en prioritering te kunnen garanderen, en de ICT-capaciteiten in lijn te brengen met de algemene organisatiebelangen
- Ga na welke mogelijkheden er bestaan om de grootste kwetsbaarheden in uw ICT-infrastructuur te verhelpen
- Raak bekend met GOVCERT – het Computer Emergency Response Team van de Nederlandse Overheid - en met wat deze organisatie voor u kan betekenen. GOVCERT heeft kennis van de concrete actuele dreigingen van cybercrime en ruime ervaring met ICT-beveiligingsincidenten. Bovendien ondersteunt GOVCERT ‘deelnemers’ die met een incident te maken krijgen. Overweeg daarom of uw organisatie deelnemer wil worden[3]
- Ga na welke mogelijkheden er (extern) zijn om cybersecurity-incidenten tijdig te detecteren en af te wenden

[2] De Handleiding Kwetsbaarheidsanalyse Spionage is een product van de AIVD en het Ministerie van Veiligheid & Justitie
[3] http://www.govcert.nl

Continuïteit inbedden
- Neem de continuïteit van uw ICT-infrastructuur mee in het continuïteitsplan van uw organisatie
  - Maak hierin duidelijk hoe de continuïteit van de ICT in het algemeen en die ten behoeve van de essentiële activiteiten in het bijzonder gestalte krijgt
  - Inventariseer welke systemen koppelingen hebben met andere interne systemen, of systemen van externe partijen. Bepaal daarbij welke verbindingen en servers vitaal zijn
  - Stel tevens vast welke cruciale knelpunten (‘single points op failure’) kunnen leiden tot de uitval van het complete systeem
  - Benoem de maximale uitvalsperiode, minimale hersteltijd van uw ICT activiteiten
  - Hanteer een afsluitprotocol zodat u weet wat te doen als u (delen van) het netwerk moet afsluiten
  - Besteed nadrukkelijk aandacht aan hoe herstel en normalisatie (‘disaster recovery’) kunnen worden bevorderd
  - Voorzie in een herstelstrategie die uitgaande van de essentiële activiteiten duidelijk maakt in welke volgorde opstart en herstel van welke systemen en voor welke personen moet plaatsvinden
  - Beschrijf tevens de noodzakelijke betrokkenheid van cruciale derden (zie verder ‘Waarborg 9: continuïteit dienstverlening derden’)

Maatregelen treffen
- Voorzie – indien uw organisatie beschikt over noodstroomvoorziening en eigen servercapaciteit – in een functionerende ‘no break’ (maatregel die de tijd tussen het uitvallen van elektriciteit en het opstarten van noodstroom overbrugt). Voorzie tevens in het testen van deze maatregel
- Voer de hardware voor de meest essentiële systemen zo redundant (‘dubbel’) mogelijk uit
- Verken de mogelijkheden tot compartimentering van uw ICT-infrastructuur en voer deze verandering door
- Identificeer en realiseer uitwijkmogelijkheden voor uw ICT-infrastructuur
- Voorzie onder uitvalsomstandigheden in het behoud van de betrouwbaarheid (integriteit) van de door uw organisatie opgeslagen data. Zie onder andere toe op het realiseren van regelmatige back ups en adequate (externe) alsmede langdurige opslag van deze data
- Draag zorg voor actuele antivirussoftware en zo up to date mogelijke virusdefinities
- Bevorder de beveiliging van systemen van externe locaties, zoals thuiswerkplekken

Waarborg 4: continuïteit elektriciteitsvoorziening

Uw organisatie is in staat om de continuïteit van elektriciteit aantoonbaar zoveel mogelijk te waarborgen. Dat geldt zowel voor de essentiële activiteiten ten behoeve van de samenleving (‘vitale diensten’) als voor andere essentiële activiteiten

Kwetsbaarheden identificeren
- Achterhaal samen met de betrokken beheerder van het elektriciteitsnet of uw organisatie vanwege de vestigingsplaats of vanwege de plaatselijke structuur van het elektriciteitsnetwerk een verhoogde kwetsbaarheid op elektriciteitsuitval vertoont
- Weet welke essentiële activiteiten op welke wijze over noodstroom moeten blijven beschikken

Weerbaarheid inventariseren
- Ga na of uw organisatie over een eigen noodstroomvoorziening beschikt

Indien uw organisatie over eigen noodstroomvoorziening beschikt:
- Weet welke delen van uw organisatie met deze voorziening van noodstroom worden voorzien en stel vast of dit in lijn is met de continuïteit van essentiële activiteiten
- Maak inzichtelijk hoe lang de voorziening in staat is om de gewenste noodstroom te leveren
- Ga na of en voor hoe lang uw organisatie over een brandstofvoorraad ten behoeve van de noodstroomvoorziening beschikt. Bedenk wat er nodig is om voor een periode van langduriger uitval over voldoende brandstof te beschikken
- Zie toe op periodiek en adequaat onderhoud van de noodstroomvoorziening
- Test de noodstroomvoorziening volgens een vaste regelmaat. Test daarbij zowel het opstarten als het daadwerkelijk voorzien van noodstroom

Strategie bepalen
- Overweeg wanneer uw organisatie nieuwbouw overdenkt of voorbereidt direct rekening te houden met een noodstroomvoorziening

Continuïteit organiseren
- Stel samen met de netbeheerder en de energieleverancier vast hoe uw organisatie onder omstandigheden van uitval zo snel mogelijk weer over stroom kan beschikken
- Overweeg om ten behoeve van ad hoc stroomvoorziening een waakvlamovereenkomst met een noodstroomleverancier af te sluiten. Houd daarbij rekening met schaarste in noodstroomvoorzieningen onder omstandigheden van grootschaliger en/of langduriger uitval

Maatregelen treffen
Indien uw organisatie niet over een eigen noodstroomvoorziening beschikt:
- Stel vast in hoeverre het niet over een eigen voorziening beschikken een expliciet en geïnformeerd besluit is geweest
- Maak een risico-inschatting van de gevolgen van elektriciteitsuitval
- Verricht in dat verlengde een kosten-baten analyse ten behoeve van noodstroomvoorziening. Houd daarbij onder meer rekening met langdurig uitval en herstel
- Ga na of en hoe een noodaggregaat effectief kan worden aangesloten. Let op: een (gehuurde) noodstroomvoorziening biedt geen garantie. Het elektriciteitssysteem van uw organisatie moet hier geschikt voor worden gemaakt (aansluitpunten, bekabeling et cetera)

Waarborg 5: continuïteit crisismanagement

Uw organisatie heeft continuïteits- en crisismanagement met elkaar verbonden. De continuïteit van het crisismanagement onder omstandigheden van uitval is aantoonbaar zoveel mogelijk gegarandeerd. De scenario's ICT- elektriciteits-uitval maken onderdeel uit van de voorbereiding op incidenten en crises

Kwetsbaarheden identificeren
- Maak de effecten voor het crisismanagement door uw organisatie onder invloed van ICT- of elektriciteitsuitval inzichtelijk
- Identificeer de gevolgen voor de alarmering van uw crisisfunctionarissen
- Identificeer of en welke ondersteunende activiteiten beschikbaar blijven als de ICT faalt
- Bepaal of en in hoeverre er informatie-uitwisseling met belanghebbenden binnen- en buiten de organisatie mogelijk zal zijn ('crisismanagement is informatiemanagement')

Weerbaarheid inventariseren
- Ga na welke onderdelen van de crisisruimte zijn aangesloten op een eventuele noodstroomvoorziening (zie verder 'Waarborg 4: continuïteit elektriciteits-voorziening') en weet voor hoe lang dit in principe het geval is

Continuïteit organiseren
- Stel bovendien vast hoe u bereikbaarheid kunt garanderen en hoe uw interne en externe partners te weten komen hoe het crisisteam te bereiken valt
- Betrek voor zover geen vast onderdeel van de crisisorganisatie standaard interne specialisten (ICT, faciliteiten, beheer). Maak de minder alledaagse verstoringen standaard onderwerp van de crisismanagementorganisatie. Garandeer bovendien dat afwegingen over continuïteit en herstel altijd in dialoog tussen de ICT-mogelijkheden en de organisatiebelangen tot stand komen.
- Garandeer betrokkenheid van die derden waarmee u een cruciale afhankelijk-heidsrelatie heeft. Met name derden die medeverantwoordelijk zijn voor uw herstel (zie verder 'Waarborg 9: continuïteit dienstverlening derden'). Maar ook relevante overheden (lokale overheden, GOVCERT e.a.). Niet alleen tijdens de response- maar ook in de voorbereidingsfase. Stem de voorbereidings-activiteiten van uw organisatie bovendien af met partnerorganisaties

Continuïteit inbedden
- Werk de scenario's ICT en elektriciteitsuitval voor uw crisisorganisatie uit. Houd hierbij nadrukkelijk rekening met de 'crisis na de crisis'. De oorzaak en de oplossing voor de uitval vormen niet meer dan het begin van herstel en normali-satie. Er zal nog geruime tijd sprake zijn van schaarste, instabiliteit et cetera
- Bereid de crisisorganisatie door middel van gerichte trainings- en oefenactivi-teiten voor op uitval van ICT of elektriciteit
- Houd bij ontruiming of evacuatie eveneens rekening met de mogelijkheid dat u niet op korte termijn kunt terugkeren. Zorg dat informatie en eventuele andere zaken die belangrijk zijn voor uw continuïteit worden meegenomen

Maatregelen treffen
- Voorzie in een uitwijkmogelijkheid (zie verder 'Waarborg 8: continuïteit werk-zaamheden en werkomstandigheden')

Waarborg 6: continuïteit communicatie

Uw organisatie is in staat om de algehele bereikbaarheid – en die van sleutel-functionarissen in het bijzonder – in het geval van ICT of elektriciteitsuitval zoveel mogelijk te garanderen. Ook zijn er door uw organisatie aantoonbaar voorbereidingen getroffen om onder deze omstandigheden interne en externe communicatie mogelijk te maken

Kwetsbaarheden identificeren
- Identificeer welke personen ten behoeve van de continuïteit van uw essentiële activiteiten (mobiel) bereikbaar moeten blijven
- Maak inzichtelijk van welke aanbieder(s) van vaste en mobiele telecomdiensten uw organisatie afhankelijk is

Weerbaarheid inventariseren
- Stel vast of uw organisatie beschikt over alternatieve telecomtoepassingen zoals satelliettelefonie
- Ga na welke interne communicatiesystemen en externe communicatiemogelijk-heden kunnen blijven functioneren op basis van noodstroomvoorzieningen. Heb hierbij in het bijzonder oog voor de crisiscommunicatiemiddelen en –behoefte (denk aan specifieke informatienummers, websites e.d.)

Strategie bepalen
- Bereid een interne- en externe communicatiestrategie voor die is gebaseerd op het gedeeltelijk of geheel ontbreken van reguliere communicatiemiddelen en gelijktijdig een toename van de informatie- en communicatiebehoefte ('infor-matieparadox')

Continuïteit organiseren
- Bereid alternatieve vormen van communicatie zo ver mogelijk voor. Maak bijvoorbeeld afspraken over het communiceren richting een bepaalde doelgroep op een vast moment vanuit een centraal verzamelpunt. Bedenk ook hoe 'klas-sieke' communicatievormen als flyeren, intercom/geluidsversterking of 'hoort zegt het voort' adequaat kunnen worden toegepast

Continuïteit inbedden
- Test de alternatieve voorlichtingsstrategie door deze te beoefenen

Maatregelen treffen
- Mocht uw organisatie beschikken over een aansluiting op het Nationaal Noodnet[4] dan is het van belang om:
  - Deze periodiek te onderhouden en te testen
  - De bekendheid met het Nationaal Noodnet onder eventuele gebruikers te bevorderen
  - Het noodnetnummer onder de aandacht te brengen van belangrijke partners

[4] Per 1 mei 2011 wordt het Nationaal Noodnet vervangen door de Nood Communicatie Voorziening (NCV)

- Ga na welke mogelijkheden er zijn om onder omstandigheden van uitval tijdelijk op een andere aanbieder over te schakelen. Indien de mogelijkheden hiertoe beperkt zijn, overweeg dan sleutelfiguren uit te rusten met alternatieven als extra simkaarten van andere aanbieders. Let wel: lang niet alle telefoontoestellen beschikken over een dergelijke functionaliteit
- Voorzie in mogelijkheden om telefoons en portofoons onder omstandigheden van uitval op te laden

Waarborg 7: continuïteit informatievoorziening

Uw organisatie heeft inzichtelijk gemaakt welke informatie er minimaal nodig is om de continuïteit van de essentiële activiteiten te kunnen waarborgen. Er zijn om in de beschikbaarheid van deze informatie te kunnen voorzien, aantoonbare continuïteitsmaatregelen getroffen

Kwetsbaarheden identificeren

- Weet welke informatie nodig is om de meest essentiële activiteiten doorgang te kunnen laten vinden

Weerbaarheid inventariseren

- Ga na of en welke van deze informatie onder omstandigheden van elektriciteits- of ICT uitval kan worden geraadpleegd
- Breng in kaart wat de mogelijkheden zijn om de integriteit van uw digitale informatie te kunnen controleren (zie verder ‘Waarborg 3: continuïteit ICT- & informatiebeveiliging’)

Maatregelen treffen

- Voorzie in de beschikbaarheid van de meest belangrijke informatie. Denk onder andere aan contactinformatie, contractinformatie, detailinformatie et cetera
- Identificeer maatregelen om de beschikbaarheid van de meest essentiële informatie onder omstandigheden van uitval zoveel mogelijk te garanderen
  - Denk aan het maken en ontsluiten van actuele back ups
  - Het opslaan en beschikbaar hebben van back ups op een andere locatie
  - De fysieke opslag van originelen
- Draag zorg dat de ICT beveiliging op orde is, zodat voorkomen wordt dat de continuïteit en toegankelijkheid van belangrijke informatie niet in het geding komt

Waarborg 8: continuïteit werkzaamheden en werkomstandigheden

Uw organisatie kan aantoonbaar voorzien in de continuïteit van werkzaamheden ten behoeve van essentiële activiteiten. Er zijn voorbereidingen getroffen om de essentiële activiteiten desnoods vanuit een uitwijklocatie te kunnen voortzetten. De betreffende werkzaamheden vinden nog steeds onder gezonde en veilige condities plaats

Kwetsbaarheden identificeren
- Maak duidelijk welke medewerkers op basis van de essentiële activiteiten in ieder geval van huis uit zouden moeten werken
- Bepaal welke gevolgen de uitval van zowel de elektriciteit als ICT zal hebben voor de gezondheids-, veiligheids- en beveiligingsituatie
- Weet welke gevolgen uitval van elektriciteit én ICT hebben voor
  - De interne hulpverlening
    - De mogelijkheden van de bedrijfshulpverleningsorganisatie (BHV)
    - De bereikbaarheid van overheidshulpdiensten
  - De interne veiligheidssituatie
    - Veiligheidssystemen (detectie en melding van brand, sprinklersystemen, bluswater)
  - De interne beveiligingssituatie
    - Beveiligingssystemen (detectie en melding van inbraak, camerabewaking)
  - Concrete maatregelen als toegangsregistratie en toegangsverlening, communicatie tussen beveiligers, cameratoezicht

Weerbaarheid inventariseren
- Ga na welke mogelijkheden er bestaan voor het handmatig uitvoeren van normaliter geautomatiseerde werkzaamheden
- Denk aan wat andere vestigingen van uw organisatie kunnen betekenen of ga met partnerorganisaties na wat u gezamenlijk kunt organiseren
- Breng de mogelijkheden voor thuiswerken in kaart. Weet onder andere welke mogelijkheden en beperkingen uw netwerk biedt voor thuiswerken. Stel vast hoeveel en welke medewerkers er maximaal op één moment tegelijkertijd gebruik kunnen maken van het bedrijfsnetwerk

Strategie bepalen
- Stel op basis van uw essentiële activiteiten de uitwijkbehoefte van uw organisatie vast
- Stel de essentiële activiteiten die elders moeten en kunnen worden uitgevoerd centraal
- Maak duidelijk onder welke omstandigheden en door wie het uitwijkbesluit genomen wordt

Continuïteit organiseren
- Bedenk op voorhand hoe u de arbeidscapaciteit die vrijvalt, zult inzetten. Spits de aandacht daarbij toe op de herallocatie van medewerkers ten behoeve van de essentiële activiteiten en een zo spoedig mogelijk herstel
- Maak inzichtelijk wat er nodig is om de uitwijk te kunnen realiseren

Continuïteit inbedden
- Breng betrokken derden op de hoogte van de uitwijk van uw essentiële activiteiten
- Vervat de uitwijkbehoefte en –mogelijkheden in een uitwijkplan. Neem hierin ook de thuiswerkmogelijkheden mee
- Test de uitwijklocatie met vaste regelmaat
- Oefen een uitwijksituatie in de praktijk en vervat de belangrijkste lessen in het uitwijkplan
- Voorzie ook voor omstandigheden van ICT- en elektriciteitsuitval in een actueel ontruimingsplan

Maatregelen treffen
- Besteed aandacht aan de gevolgen van elektriciteitsuitval voor:
  - De luchtzuiveringssystemen en daarmee de luchtkwaliteit
  - Het systeem voor klimaatbeheersing (reguleren van warmte of kou)
  - De drinkwatervoorziening
  - Mogelijke valrisico’s die door de duisternis kunnen ontstaan
  - Medewerkers, bezoekers of derden die vast komen te zitten in liften
- Stel vast welke aanvullende gezondheids-, veiligheids-, en beveiligingsmaatregelen u moet nemen om uw essentiële activiteiten doorgang te kunnen laten vinden óf aanvullende bescherming te bieden

Waarborg 9: continuïteit dienstverlening derden

Uw organisatie stuurt aantoonbaar op de continuïteit van de dienstverlening door ‘cruciale derden’. Derden zijn in staat om op elk gewenst moment duidelijk te maken wat zij doen om de dienstverlening te continueren. Bovendien stellen cruciale derden alles in het werk om de continuïteit van uw organisatie zo lang en goed mogelijk te waarborgen

Kwetsbaarheden identificeren
- Bepaal van welke derden (leveranciers, onderhoudsbedrijven, ondersteuners, adviseurs, afnemers) u voor het voortzetten of snel herstellen van uw essentiële activiteiten het meest afhankelijk bent
- Weet wat deze partijen doen om hun continuïteit ten behoeve van de dienstverlening aan uw organisatie te garanderen. Stel vast of dit wat u betreft voldoende zekerheden biedt

Continuïteit inbedden
- Verzoek uw cruciale derden tot het opstellen van een plan en het treffen van bijbehorende maatregelen om zowel uw continuïteit als een zo snel mogelijk herstel van deze te kunnen garanderen – in termen van zo snel mogelijke inzet van de benodigde expertise en mankracht
- Vervat de eisen die uw organisatie ten behoeve van de continuïteit stelt aan cruciale derden (leveringszekerheid, onderhoud, herstel) in contracten en service level agreements (zogenoemde SLA’s)
- Gebruik de mogelijkheid van inspectie, controle of auditing op continuïteitsvoorzieningen van uw cruciale derden en neem deze eveneens op in de overeenkomsten met deze partijen
- Vereis dat derden de maatregelen ten behoeve van de continuïteit van uw organisatie – bij voorkeur ook samen met u – testen, verslag uitbrengen over de resultaten en verbeteringen doorvoeren

Maatregelen treffen
- Ontwikkel een netwerkkaart die inzichtelijk maakt welke organisaties hinder kunnen ondervinden van een verstoring van uw continuïteit en vice versa

Waarborg 10: continuïteit financiële positie, betalingsverkeer & herstelkosten

Uw organisatie heeft bedrijfseconomische voorzieningen getroffen om de continuïteit van de essentiële activiteiten te kunnen garanderen. Uw organisatie kan inzichtelijk maken dat de meest cruciale betalingen voortgezet kunnen worden. Ook is er voldoende financiële buffer c.q. zijn er reserveringen gemaakt om de kosten ten behoeve van uitval en herstel te kunnen opvangen

Kwetsbaarheden identificeren
- Ga na wat de gevolgen van uitblijvende betalingen aan uw organisatie kunnen zijn en stel vast of en op welke termijn deze uw financiële positie zouden kunnen bedreigen
- Weet wat voor de continuïteit van uw essentiële activiteiten de meest cruciale betalingsverplichtingen van uw organisatie zijn
- Identificeer of en in hoeverre uw organisatie onder omstandigheden van uitval nog aan deze verplichtingen tegemoet kan komen
- Stel vast in hoeverre uw organisatie aansprakelijkheidsrisico’s loopt

Weerbaarheid inventariseren
- Ga na welke risico’s verzekerd zijn of nog verzekerd kunnen worden

Continuïteit organiseren
- Voorzie erin dat uw financiële positie u in staat stelt om de essentiële activiteiten te kunnen blijven uitvoeren

Maatregelen treffen
- Tref maatregelen om de meest essentiële betalingen te kunnen blijven verrichten
- Tref financiële voorzieningen om de aanvullende – snel en hoog oplopende kosten – ten behoeve van het herstel te kunnen ondervangen

Dit hulpmiddel is een uitgave van:

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Veiligheid

www.nationale-veiligheid.nl

Schedeldoekshaven 200
Postbus 20011 | 2500 EA Den Haag