

CEO-FRAUDE

CATEGORIE: IT (malware)



 In samenwerking met:



# CEO-fraude

**Disclaimer**

De informatie in dit document is bedoeld om de werkgever stof tot nadenken te geven in het kader van incidentenbeheer om de bedrijfscontinuïteit te verzekeren. Het is dus niet de bedoeling om autoriteiten die verantwoordelijk zijn voor het toezicht op de veiligheid op het werk te vervangen. Deze informatie ontslaat de werkgever niet van de verplichting om zich te houden aan de reglementaire bepalingen die van toepassing kunnen zijn op elke specifieke werksituatie.

Dit betekent dat het gebruik van dit document door de werkgever altijd afhankelijk is van zijn pragmatisch oordeel en dat het aan hem is om de elementen en omstandigheden te beoordelen, zowel in feite als in rechte, waarmee de werkgever in welomschreven en concrete gevallen op de werkplek te maken krijgt.

Voor interpretaties in concrete gevallen of situaties kan altijd het advies worden ingewonnen van de ambtenaren die verantwoordelijk zijn voor het toezicht op de arbeidsveiligheidsvoorschriften.

*Voor meer informatie over de verschillende stappen, zie het “Incidentenbeheerplan”, hoofdstuk III.*

CEO-Fraude

[I. Stap 1: Voorbereiding (voor het incident) 5](#_Toc57728869)

[1.1: Kies iemand die aan het roer staat 5](#_Toc57728870)

[1.2: Ken uw risico’s 5](#_Toc57728871)

[1.3: Preventieve maatregelen 7](#_Toc57728872)

[II.Stap 2: Melding en identificatie 11](#_Toc57728876)

[2.1: Melding 11](#_Toc57728877)

[2.2: Identificatie 11](#_Toc57728878)

[III.Stap 3: Activering en behandeling (incident) 12](#_Toc57728882)

[3.1: Identificeer uw instrumenten en middelen 12](#_Toc57728883)

[3.2: **BEHEERSMAATREGELEN** 13](#_Toc57728884)

[IV.Stap 4: Eradication 14](#_Toc57728885)

[V.Stap 5: Deactivering 14](#_Toc57728886)

[VI.Stap 6: Geleerde lessen (post incident review) (NA HET INCIDENT) 15](#_Toc57728887)

[6.1: Context : verzamel de juiste informatie 15](#_Toc57728888)

[6.2: Evaluatie van het incident en geleerde lessen 15](#_Toc57728889)

[VII.Bijlagen 19](#_Toc57728890)

[7.1: Contactenlijst 19](#_Toc57728891)

[7.2: Tabel 21](#_Toc57728892)

1. Stap 1: Voorbereiding (VOOR HET INCIDENT)

Zie Risk Assessment et Risk Treatment.

### 1.1: Kies iemand die aan het roer staat

|  |
| --- |
| **Wie kan dit incidentenbeheerplan opstellen ?**  **Wie kan dit plan valideren (management)?** |

*Zie Bijlage VII, 7.2: Tabel*

In grote bedrijven kan een groep (idealiter multidisciplinair en inclusief) worden gevormd.

In kleinere bedrijven kan één en dezelfde persoon door het management worden aangesteld of kan het management zelf deze rol op zich nemen. In dit geval is het echter raadzaam om een back-up aan te wijzen (een persoon die hem/haar kan vervangen in geval van afwezigheid, ziekte of vertrek).

Vergeet niet uw interne of externe IT-dienst als u die heeft.

Zorg ervoor dat u de procedures/het incidentbeheerplan laat valideren, alsook het huidige document

### 1.2: Ken uw risico’s

|  |
| --- |
| **Heeft u een Risk Assessment gerealiseerd ?**  **Heeft u een Risk Treatment gerealiseerd ?** |

*Zie Bijlage VII, 7.2: Tabel*

Opdat het incidentenbeheerplan effectief zou zijn, moet het bedrijf haar risico's hebben geïdentificeerd, geanalyseerd en geëvalueerd. Dit is het doel van de Risk Assessment (zie template). Het is ook noodzakelijk dat de maatregelen voor het behandelen van deze risico’s gekend zijn, dit is het doel van de Risk Treatment (zie template).

U moet ook specifieke scenario’s identificeren.

**Scenario :**

CEO-fraude is een meer geavanceerdere en sluwere vorm van phishing (het valt onder de noemer “*spear phishing*”). De oplichter heeft in dit geval het bedrijf eerst grondig bestudeerd en hij weet tot op een bepaalde hoogte hoe het bedrijf georganiseerd is en functioneert. Vervolgens doet hij zich voor als de CEO (of iemand met een gezaghebbende functie) en contacteert hij via een vals of gehackt e-mailadres (of via de telefoon) specifieke personen binnen het bedrijf met de bedoeling om dringend geld over te maken of gevoelige gegevens mee te delen. Daarom zijn de financiële verantwoordelijken vaak het doelwit van CEO-fraude , maar evengoed kunnen de personeels- of IT-diensten het slachtoffer zijn of zelfs andere senior managers! Dit laatste geval noemt men ook wel eens “*whaling*”: men probeert een “walvis” in de val te lokken i.p.v. een kleine vis.

Een onoplettende werknemer gelooft dat hij gecontacteerd werd door de CEO van het bedrijf waarvoor hij/zij werkt en geconfronteerd met diens autoriteit, gehoorzaamt hij/zij en voert de opdracht nietsvermoedend uit.

**Van**: De CEO <debigboss@uwbedrijf.com>

**Verzonden**: 09 oktober 2020 om 11:06

**Aan**: De boekhoudafdeling van uw bedrijf <Peter.Deboekhouder@uwbedrijf.com>

**Onderwerp**: DRINGEND: Uit te voeren betaling

Hallo Peter,

Kan je me een plezier doen, a.u.b.? Ik heb zojuist een herinnering ontvangen van een van onze leveranciers dat we hen nog een achterstallige betaling moeten en dat ze sancties zullen opleggen als het bedrijf vandaag niet betaalt. Aangezien ik vandaag de hele dag in een externe vergadering zit, zal ik onbereikbaar zijn en kan ik het niet vanaf hier afhandelen. Kan je snel het nodige doen a.u.b.? Ik heb ze gezegd dat ze je direct kunnen contacteren via e-mail (bedrijf XX). Vergeet niet om ook je map ongewenste na te kijken, *just in case* de mail daar terecht zou komen). Je kan ook anders ook betalen door op de link hier te klikken en het aangegeven bedrag over te maken.

Dit moet met prioriteit VANDAAG gebeuren.

Ik weet dat ik op je kan rekenen.

Als je een vraag zou hebben, kan je reageren via deze e-mail, want zoals aangegeven ben ik vandaag niet telefonisch bereikbaar...

Bedankt!

De CEO

**Risico's :**

Meestal is er sprake van een financieel verlies, maar evengoed kan er een verlies zijn van persoonlijke of bedrijfsgegevens, reputatieschade,… Hoewel minder voorkomend, kan er ook malware geïnstalleerd worden.

### 1.3: Preventieve maatregelen

#### Technisch

Hoewel CEO-fraude een meer geavanceerde vorm is van phishing, kunnen dezelfde technische verdedigingsmechanismen ook hier hulp bieden.

Vraag steeds **advies aan uw IT-verantwoordelijke** (intern of extern), indien uw bedrijf hierover beschikt. Zij kunnen u bijstaan met advies omtrent nuttige technische applicaties die u kunt gebruiken bij het verdedigen van uw bedrijf.

Hieronder kunt u alvast enkele goede praktijken vinden.

* Gebruik een **beveiligde e-mailgateway** (“secured email gateway of SEG”).
* Binnenkomende en uitgaande e-mails worden zo gefilterd op phishing, spam, malware, … De kans dat een phishingmail nog in de inbox terechtkomt, wordt zo drastisch verminderd. Enkele gekende leveranciers zijn cisco, IBM, citrix,…
* Schakel de **voorbeeldweergave** van bijlagen en weergave van afbeeldingen uit.
* Bijlagen en afbeeldingen kunnen schadelijk zijn! Het is niet omdat een e-mail afbeeldingen bevat dat deze ook effectief zich in deze mail bevinden. Een afbeelding maakt namelijk niet altijd automatisch onderdeel uit van een e-mail, maar wordt meestal via een verborgen link (URL) gedownload. Deze verborgen links kunnen een toegangspoort vormen voor cyberaanvallers. Bovendien geeft u door het downloaden van een afbeelding aan dat het e-mailadres nog in gebruik is, waardoor u zich aan nog meer phishingmails/spam kunt verwachten.
* Voer **een sterk paswoordbeleid** of nog beter: gebruik een **Multifactorauthenticatie (MFA)** waar het kan voor het inloggen op uw rekeningen en systemen.
* In plaats van enkel gebruik te maken van een standaard loginnaam + wachtwoord, kunt u vragen om extra factoren te gebruiken om in te loggen. Dit kan gaan van het verzenden van een simpele sms naar een vertrouwde gsm/smartphone in uw bezit, tot het gebruik maken van biometrische gegevens zoals vingerafdrukken of gezichtsherkenning. Een bekend voorbeeld hiervan is “Itsme”. Door gebruik te maken van een authenticatie met meerdere factoren, vermindert u de kansen dat een phisher die over uw wachtwoord zou beschikken, deze ook effectief deze kan gebruiken, want hij beschikt niet over de andere factoren.
* **Zoals steeds: rekening houden met volgende vuistregels voor een goede cyberhygiëne:**

#### Organisatorisch

CEO-fraude kan net als een gewone phishingaanval pas slagen als de mensen ook effectief in de val trappen. Alleen is het bij CEO-fraude veel moeilijker om in één oogopslag te zien dat er iets niet klopt, aangezien de oplichter zich grondig voorbereid heeft om geloofwaardig over te komen. Ook hier is **sensibiliseren én testen van álle werknemers dus essentieel**! Specifieke aandacht moet hierbij gaan naar het managementniveau, niet enkel omdat zij een mogelijk doelwit vormen, maar ook omdat het veelal in hun naam zal zijn dat de CEO-fraude zal plaatsvinden. Elke werknemer moet met een kritische blik een mail kunnen bekijken en niet zomaar blind gevolg geven aan vreemde en onverwachte opdrachten. (zie ook fiche phishing).

CEO-fraude is sluwer dan de gewone cliché phishingaanval. Spellingsfouten zullen veelal niet aanwezig zijn en ook zal men zich voordoen als een bekende binnen het bedrijf en misbruik maken van de autoriteit van die persoon.

**Toch zijn er enkele typische kenmerken**:

* De boodschap blijft dringend
  + er moet snel geld overgeschreven worden of gevoelige informatie prijs worden gegeven, liefst vandaag nog
* De opdracht is in strijd met de vastgelegde interne procedures
  + De opdracht moet meestal vertrouwelijk blijven: het gaat om een verrassing, een prestigieus geheim project, een project met verzwegen moeilijkheden,…
* De CEO (of een andere persoon met een gezagsfunctie) stelt dat hij toevallig vastzit in een vergadering of niet aanwezig is op bureau en het dus niet zelf kan doen
  + De CEO rekent specifiek op u om de opdracht tot een goed einde uit te voeren en plaatst druk op u
  + U zou de CEO een grote dienst bewijzen of omgekeerd: risico op sancties indien u geen gevolg geeft aan de opdracht
  + Er wordt gevraagd om niet te telefoneren en slechts te reageren op het gebruikte e-mailadres (of helemaal niet te reageren)
* De CEO stelt dat een vertrouwende leverancier betaald moet worden, maar de betaling dient te gebeuren op een nieuw bankrekeningnummer
  + De CEO stelt dat een persoon, bv. een advocaat u telefonisch zal contacteren met betrekking tot een dringende zaak
* De CEO heeft u nog nooit rechtstreeks gecontacteerd of nog nooit een gelijkaardige opdracht van u gevraagd

Bekijk het e-mailadres!

Het e-mailadres ziet er vreemd uit, is u niet bekend of is met zorg opgesteld. Zweef met de muiscursor over het adres van de afzender om deze volledig te bekijken! Zaken waar op gelet moet worden:

* De afzender lijkt uw CEO te zijn, maar het eigenlijke e-mailadres is afkomstig van buiten de onderneming, bv. CEO@gmail.com, CEO@hotmail.com,... in plaats van CEO@uwbedrijf.be
* Het e-mailadres stemt perfect overeen, afgezien van een kleine wijziging in de domeinnaam, bv. CEO@uwbedijf.be (zonder “r”) in plaats van CEO@uwbedrijf.be of bv. de letter “l” is vervangen door een hoofdletter “i”.
* Maar het e-mailadres kan ook perfect overeenstemmen
  + Omdat het vervalst is (in jargon: “*spoofing*”). Antwoorden worden dan meestal omgeleid naar een ander e-mailadres (het reply-to adres zal hier verschillen). In principe houdt een goede beveiligde e-mailgateway dergelijke mails tegen.
  + Ofwel omdat het effectieve e-mailadres van de CEO gehackt is, wat des te zorgwekkender is.
* Het is **ok om te twijfelen** of een mail vals is of echt!
  + **Contacteer rechtstreeks de CEO (of zijn/haar diensten)** (via andere officiële kanalen, niet door te antwoorden op de mail), zo bent u onmiddellijk zeker of de mail echt of vals is
* **Deel geen interne info** (beveiliging, procedures, interne organisatie,…) met anderen buiten het bedrijf (ook niet op sociale media)
* Zie ook de fiche phishing voor meer algemene kenmerken van phishingmails

**Specifiek voor het managementniveau kunnen volgende tips helpen:**

* Installeer een **beleid omtrent communicatiemethoden** binnen uw bedrijf voor officiële communicatie en het uitvoeren van opdrachten.
  + Zo kan bv. vereist worden dat men steeds het bedrijfsaccount moet gebruiken voor het verzenden van e-mails en dat aan alle e-mails van medewerkers die vanuit een vreemd e-mailadres sturen, geen gevolg mag worden gegeven
  + Spreek ook duidelijk af met **leveranciers/cliënteel** wat de officiële communicatiekanalen zijn. CEO-fraude gebeurt niet enkel binnen het bedrijf! Ook uw leveranciers/cliënteel kunnen gecontacteerd worden met de vraag om een bepaalde opdracht uit te voeren die afwijkt van de normale gang van zaken .
* Installeer een **beleid voor het uitvoeren van betalingen**.
  + Zorg ervoor dat betalingen nooit kunnen gebeuren o.b.v. een simpele mail van een hiërarchische meerdere, maar dat hieraan officiële procedures verbonden zijn en onderworpen zijn aan meerdere controles en goedkeuringen (zeker voor wat betreft grote bedragen).
* Zorg ervoor dat er **geen angstcultuur** heerst binnen het bedrijf.
  + Elke aanval of incident moet zo snel mogelijk gemeld, zonder dat men angst moet hebben dat men hierop afgerekend zal worden. Hoe langer een incident onder de radar blijft, hoe groter de potentiële schade kan zijn voor het bedrijf.
  + Overweeg een centraal meldpunt
* **Controleer regelmatig uw bankuitgaven** om er zeker van te zijn dat er geen verdachte handelingen gebeuren.
* Evalueer of het voor uw bedrijf voordelig kan zijn om eventueel een **cyberverzekering** af te sluiten, die de potentiële schade kan dekken.

**Denk eraan om regelmatig oefeningen te organiseren**. Het verwerven en onderhouden van goede reflexen vereist regelmatige oefeningen. Bovendien is het vaak dankzij deze oefeningen dat het bedrijf zich realiseert dat de gegevens niet meer actueel zijn (contactnummers die niet meer geldig zijn, contracten die verlopen zijn, enz....), dat nieuwe medewerkers nog niet zijn opgeleid, dat de software niet up-to-date is,... En waarom niet een "nep-phishing" organiseren? U zou uw personeel kunnen verrassen, zien "wie er in trapt" en hoe u het bewustzijn van uw personeel kunt vergroten. Het is natuurlijk niet de bedoeling om degenen die er voor vallen te straffen, iedereen kan een fout maken, het belangrijkste is om te leren en bewust te zijn

Nuttige links

* CEO-fraude herkennen: [Cert.be](https://cert.be/nl/paper/ceo-fraude-beter-voorkomen-dan-betalen); [Febelfin](https://www.febelfin.be/nl/dossiers/hoe-voorkom-je-ceo-fraude); [federale politie](https://www.politie.be/5998/nl/nieuws/ceo-fraude), [dnsbelgium](https://www.dnsbelgium.be/nl/nieuws/pas-op-voor-ceo-fraude)
* Phishing herkennen: [Safeonweb](https://safeonweb.be/nl/leer-valse-mails-herkennen), incl [phishingtest](https://safeonweb.be/nl/quiz/phishingtest); [Febelfin](https://www.febelfin.be/nl/consumenten/artikel/phishing-dit-hoe-jij-meteen-een-fake-bericht-herkent); [FOD Binnenlandse zaken](https://www.besafe.be/nl/veiligheidsthemas/cyberveiligheid/cybercriminaliteit/phishing)
* Sensibiliseren met de [Cyber Security KIT](https://www.cybersecuritycoalition.be/nl/resource/cyber-security-kit/) van de Cyber Security Coalition
* Multifactorauthenticatie: [Cyber Security Coalition](https://www.cybersecuritycoalition.be/nl/resource/wachtwoorden-niet-meer-tijd/) & [Safeonweb](https://www.safeonweb.be/index.php/nl/tweestapsverificatie-toevoegen-hoe-doe-ik-dat)
* De site van het [Centrum voor Cybersecurity België](https://ccb.belgium.be/nl) (CCB)
* Spoofing: [Safeonweb](https://www.safeonweb.be/nl/help-eigen-mailadres-als-afzender-spoofing)

1. Stap 2: Melding en identificatie

### 2.1: Melding

Het is essentieel om een incident snel te kunnen opsporen, identificeren en kwalificeren/classificeren om de impact op de continuïteit van de activiteiten te beperken door de juiste procedure te Activering. De persoon die de melding van het incident ontvangt, kwalificeert het incident op van vooraf vastgestelde criteria.

Elke werknemer moet elk incident of gebeurtenis die tot een incident kan leiden, zo snel mogelijk melden. Klanten en leveranciers kunnen ook een incident melden.

De middelen om incidenten te melden zijn beschreven in het incidentenbeheerplan.

* Zie Stap 3: Activering en behandeling, beheersmaatregelen

### 2.2: Identificatie

2.2.1: Identificeer de betrokken activiteiten

|  |
| --- |
| **Wat zijn de taken van het bedrijf die behouden moeten blijven om haar economische overleving te verzekeren?**  **Zie ook het Business Continuity plan (BCP) en de vastgelegde tijdsdoelstellingen (RTO,…)** |

Om u te helpen uw processen en activiteiten te prioriteren, stelt u zich de volgende vragen:

1. welke activiteiten zouden het personeel (of de klanten,...) in gevaar kunnen brengen?
2. welke activiteiten kunnen na enkele uren een ernstige economische impact hebben op het bedrijf? Na 24u? 48u? Een week?

**LIJST MET ESSENTIELE ACTIVITEITEN**

| **Essentiële activiteit 1** |
| --- |
| Sleutelpersoneel |
| Belangrijke informatie of gegevens |
| Noodzakelijke IT-diensten (hardware, software) |
| Gebouwen |
| Externe contactpersonen (ressources) |
| Onderlinge afhankelijkheid (interdependentie) met andere activiteiten (zo ja, welke) |
| ... |

2.2.2: Classificeer

De persoon die de informatie ontvangt (bv. Helpdesk) dient deze bijvoorbeeld als volgt in te delen:

1. **Zwak** - er hebben zich geen incidenten voorgedaan, maar de gebeurtenis houdt verband met een systeem, proces of organisatie en kan een incident in de nabije of toekomstige toekomst veroorzaken;
2. **Klein** - een incident dat geen significante impact heeft op de bedrijfscontinuïteit;
3. **Groot** - een incident dat een significante impact kan hebben op de organisatie, maar nog niet als een crisis wordt beschouwd;
4. **Crisis** - een incident dat een aanzienlijke impact kan hebben op de organisatie en de bedrijfscontinuïteit.

2.2.3: Identificeer de prioriteiten

|  |
| --- |
| **In geval van onderbreking of achteruitgang van uw activiteiten, wat is de prioriteitsvolgorde van de activiteiten?**  **Wat zijn uw tijdsdoelstellingen?**  **Zie ook de Risk Assessment, Risk Treatment en het Business Continuity Plan** |

Bij het analyseren van de impact op de bedrijfscontinuïteit moet u er rekening mee houden dat niet alle activiteiten noodzakelijkerwijs voor 100% werken, maar dat dit aanvaardbaar kan zijn.

Heeft u uw prioritaire activiteiten gedefinieerd? Nu gaat het erom de volgorde te bepalen waarin deze activiteiten moeten worden hervat (sommige diensten zijn onderling afhankelijk van andere) en de geschatte tijdsdoelstellingen te identificeren door ze te vergelijken met de vastgelegde doelstellingen (zie Risk Assessment en Business Continuity Plan).

Op basis van het bovenstaande, is het een kwestie van het bepalen in welke volgorde maatregelen moeten worden genomen om de continuïteit van essentiële activiteiten te waarborgen. Denk eraan de mogelijke onderlinge afhankelijkheid van bepaalde activiteiten te overwegen en een permanente dialoog met de beheerder van het Business Continuity Plan te onderhouden

1. Stap 3: Activering en behandeling (INCIDENT)

Het hoofddoel is om de impact van het incident op de bescherming van het menselijk leven en de continuïteit van de activiteiten van het bedrijf zo snel mogelijk te verminderen.

### 3.1: Identificeer uw instrumenten en middelen

*Zie bijlage VII, punt 7.2: Tabel*

In het bijzonder uw procedures (identificatie,...), uw communicatiemiddelen,...

### 3.2: BEHEERSMAATREGELEN

**EEN E-MAIL ONTVANGEN VAN DE “CEO”?**

|  |  |
| --- | --- |
|  | Controleer de e-mail en vooral het e-mailadres op echtheid, klik nergens op! |
|  | Contacteer de CEO of dienst diensten via de normale communicatiekanalen en vraag om bevestiging |
|  | Indien vals bericht: beantwoord de mail niet, geef geen enkel gevolg aan de mail! Duid de valse afzender aan als ongewenst en blokkeer deze |

|  |  |
| --- | --- |
|  | Breng de rest van het bedrijf op de hoogte zodat niemand in de val loopt |
|  | Meld de poging bij   * + het [CERT.be](https://cert.be/nl/een-incident-melden-form) of via [cert@cert.be](mailto:cert@cert.be).   + de lokale politie, ook poging tot fraude is strafbaar! |
|  | Verwijder de mail |

**TOCH IN DE VAL GETRAPT?**

|  |  |
| --- | --- |
|  | Breng de verantwoordelijken op de hoogte |
|  | Contacteer:   * Indien u geld heeft overgemaakt: contacteer zo snel mogelijk uw bank! Mogelijk is er nog tijd om de transactie te blokkeren of een annulatie te vragen * dien klacht in bij de lokale politie * Indien u een cyberverzekering heeft afgesloten en u heeft schade opgelopen: contacteer u verzekeringsmakelaar * Indien er persoonsgegevens gelekt zouden zijn (“*data breach*”), bent u verplicht om **binnen de 72 uur** de [Gegevensbeschermingsautoriteit](https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens) te contacteren |
|  | Laat de IT-verantwoordelijke(n) (intern of extern) een antivirusscan uitvoeren, controleer ook, na akkoord, de mailbox van de CEO |
|  | Breng de rest van het bedrijf op de hoogte zodat niemand anders in de val loopt |
|  | Wijzig uw wachtwoord(en) |
|  | Wijzig ook alle gevoelige info die u eventueel heeft doorgegeven (indien mogelijk) |
|  | Meld de CEO-fraude bij het [CERT.be](https://cert.be/nl/een-incident-melden-form) of via [cert@cert.be](mailto:cert@cert.be) |
|  | Duid de valse afzender aan als ongewenst en blokkeer deze |
|  | Verwijder de mail pas van zodra u zeker bent dat u geen schade heeft geleden en deze niet langer als bewijsmateriaal dient |

1. Stap 4: Eradication

Het is niet altijd mogelijk om de oorzaken van het incident tijdens het incident zelf vast te stellen. In dit geval moeten eerst de gevolgen (impact op de bedrijfscontinuïteit) worden aangepakt voordat de oorzaak kan worden vastgesteld. Er moeten echter redelijke inspanningen worden geleverd om de oorzaak te achterhalen en het risico te beperken dat een dergelijk incident zich opnieuw voordoet.

1. Stap 5: Deactivering

Wanneer de diensten die door een incident werden getroffen, weer normaal functioneren, kan het incident worden afgesloten door het team dat het incident opvolgde (bv. helpdesk) in overeenstemming met de beheerder van het Business Continuity Plan.

Het incidentenbeheerplan wordt gedeactiveerd en er wordt een "Post Incident Review" uitgevoerd (zie stap 6).

De volgende acties moeten worden ondernomen:

| **Actie** | **Functie** | **Verwijzingen naar andere documenten**  **Naam en referentie** |
| --- | --- | --- |
| Afsluiten van het incidententicket | Helpdesk na akkoord van de beheerder van het incidentenbeheerplan | Ticket in het kader van incidentenbeheer |
| Deactiveren incidentenbeheerplan | Beheerder incidentenbeheerplan |  |
| Post Incident Review | Beheerder incidentenbeheerplan | Post Incident Review (document) |
| … |  |  |

1. Stap 6: Geleerde lessen (Post Incident Review) (NA HET INCIDENT)

*“I never lose. I either win or learn.”*

Nelson Mandela

Het doel is om te leren uit de ervaring door een "Post Incident Review" uit te voeren en zo het incidentenbeheer via een continu proces te verbeteren.

De Post Incident Review zou ten minste de volgende elementen moeten bevatten :

### 6.1: Context : verzamel de juiste informatie

| **Element** | **Informatie** |
| --- | --- |
| **Administratie** |  |
| Incidentnummer in het incidentlogboek: |  |
| Datum en tijd waarop het incident werd vastgesteld: |  |
| Datum en tijd waarop het incident werd opgelost: |  |
| Type incident: |  |
| Ernst van het incident: |  |
| Was er impact voor klanten: |  |
| Wie was beheerder van het incident: |  |
| Beschrijving van het incident: |  |
| … |  |

### 6.2: Evaluatie van het incident en geleerde lessen

|  |  |
| --- | --- |
| **Detectie** |  |
| Wie stelde het incident vast en hoe: |  |
| Werd het incident tijdig opgemerkt of had het eerder ontdekt kunnen worden: |  |
| Kunnen procedures of tools helpen om dit soort incidenten nog vroeger op te sporen: |  |
| Werden de juiste meldingsprocedures gevolgd: |  |
| … |  |

|  |  |
| --- | --- |
| **Beoordeling en acties** |  |
| Werd het incident correct ingeschat: |  |
| Was de hiervoor nodige informatie beschikbaar: |  |
| Werd het BCP geactiveerd: |  |
| Welke andere acties werden ondernomen om het incident op te lossen: |  |
| Welke resources werden gebruikt om het incident te beheren: |  |
| Is het plan flexibel genoeg om met onvoorziene events om te kunnen gaan: |  |
| Werden de acties tijdig ondernomen: |  |
| … |  |

|  |  |
| --- | --- |
| **Communicatie** |  |
| Werd er (tijdig) intern gecommuniceerd: |  |
| Werd er (tijdig) extern gecommuniceerd: |  |
| Welke communicatiekanalen werden ingezet: |  |
| Wanneer werd de eerste communicatie uitgestuurd en hoe regelmatig werd deze geüpdatet: |  |
| Werden de juiste personen betrokken: |  |
| Welke communicatie was nuttig: |  |
| Welke communicatie bleek inefficiënt: |  |
| … |  |

|  |  |
| --- | --- |
| **Analyse van de oorzaak** |  |
| Werd de oorzaak van het incident vastgesteld: |  |
| Zijn er verwante of soortgelijke incidenten vastgesteld: |  |
| Is er een onderliggend probleem: |  |
| Is er extra actie nodig om het onderliggende probleem te identificeren (zie stap 4 Eradication): |  |
| … |  |

|  |  |
| --- | --- |
| **Preventie** |  |
| Wat kunnen we leren uit de gebeurtenis: |  |
| Hoe kunnen we vermijden dat een soortgelijk incident zich opnieuw voordoet, en wie moet hiervoor actie ondernemen: |  |
| … |  |

|  |  |
| --- | --- |
| **Gepastheid van de reactie** |  |
| Effectieve hersteltijd (vergelijk met Recovery Time Objective – RTO)  Het incident werd binnen de vooropgestelde tijd opgelost:  Voor geen van de activiteiten  Slechts voor enkele activiteiten  Voor alle activiteiten |  |
| Moeten er contracten aangepast worden: |  |
| … |  |

|  |  |
| --- | --- |
| **Hoe reageerde het management op het incident** |  |
| Management reageerde niet of onvoldoende |  |
| Management reageerde, maar volgde de plannen niet volledig |  |
| Management reageerde volledig volgens de plannen |  |
| … |  |

|  |  |
| --- | --- |
| **Mate waarin het personeel voorbereid was op het incident** |  |
| 1. Onvoorbereid |  |
| 2. Deels voorbereid |  |
| 3. Volledig voorbereid |  |
| … |  |

|  |  |
| --- | --- |
| **Gewenste verbeteringen** |  |
| Wat zou kunnen bijgestuurd worden om het incident in de toekomst sneller op te lossen: |  |
| … |  |

|  |  |
| --- | --- |
| **Schadeclaims** |  |
| Zijn er schadeclaims: |  |
| Werden schadeclaims ingediend bij derden in verband met dit incident: |  |
| … |  |

|  |  |
| --- | --- |
| **Varia** |  |
| … |  |

1. Bijlagen

### 7.1: Contactenlijst

**INTERNE CONTACTEN**

| **Functie** | **Voornaam NAAM**  ***Denk eraan om ook een andere persoon aan te duiden in geval van afwezigheid, ziekte,... van de referentiepersoon.*** | **Actie** | **Contactgegevens**  ***Vaste telefoon***  ***Bureau***  ***Thuis***  ***Mobiel***  ***E-mail***  ***Voorkeuren voor contact (snelste)*** |
| --- | --- | --- | --- |
| Referentiepersoon (bedrijfscontinuïteit) |  |  |  |
| Alternatief |  |  |  |
| ... |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**EXTERNE CONTACTEN**

| **Functie** | **Voornaam NAAM**  ***Denk eraan om ook een andere persoon aan te duiden in geval van afwezigheid, ziekte,... van de referentiepersoon..*** | **Contract**  ***Referentie*** | **Contactgegevens**  ***Vaste telefoon***  ***Bureau***  ***Thuis***  ***Mobiel***  ***E-mail***  ***Voorkeuren voor contact (snelste)*** |
| --- | --- | --- | --- |
| Verzekeraar |  |  | Vaste telefoon  Bureau  1)  2)  Thuis  1)  2)  Mobiel  1)  2)  E-mail  1)  2) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 7.2: Tabel

|  |  |  |
| --- | --- | --- |
| **1.1: Kies iemand die aan het roer staat** | **Functieomschrijving van wie de taak uitvoert** | **Welke procedures moeten gevolgd worden?** |
|
| [Scenario 1] |  |  |
| [Scenario 2] |  |  |
| […] |  |  |

|  |  |  |
| --- | --- | --- |
| **1.2: Ken uw risico’s** | **Herneem het resultaat uit kolom P van de Risk Assessment (2 (groen) tot 10 (rood))** | **Focusgroep?** **(1 of 2)** |
| O.b.v. uw risk assessment, wat is uw risiconiveau in scenario 1? |  |  |
| O.b.v. uw risk assessment, wat is uw risiconiveau in scenario 2? |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **2.2.3: Identificeer de prioriteiten**   * Wat zijn uw tijdsdoelstellingen? * Wat is de maximale "aanvaardbare" tijd voor u om de werking van de activiteit te herstellen? (Recovery Time Objective of RTO) * Wat is de maximale leeftijd van de gegevens die u nodig heeft om te herstellen (Recovery Point Objective of RPO) * Wat heeft u met uw leveranciers afgesproken (Recovery Consistency Objective of RCO)? * … in geval van onderbreking of verslechtering van uw activiteiten, wat is de prioriteitsorde van de activiteiten (P)? | | | |
| **2.2.1: Identificeer de betrokken activiteiten** |  | | **RTO** | **RPO** | **RCO** | **P** |
| Mensen |  | |  |  |  |  |
| Infrastructuur |  | |  |  |  |  |
| Technologie |  | |  |  |  |  |
| Informatie en documentatie |  | |  |  |  |  |
| Derden |  | |  |  |  |  |
| … |  | |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **3.1: Identificeer uw instrumenten en middelen** | **Essentiële activiteit 1** | **Essentiële activiteit 2** |
| Sleutelpersoneel |  |  |
| Belangrijke informatie of gegevens |  |  |
| Noodzakelijke IT-diensten (hardware, software) |  |  |
| Gebouwen |  |  |
| Externe contactpersonen (middelen) |  |  |
| Interdependentie met andere activiteiten (zo ja, welke) |  |  |
| **…** |  |  |