Handleiding en draaiboek opzetten cybercrisisoefeningen

gebaseerd op cybercrisisoefening OZON

Utrecht, april 2017

Colofon

Handleiding en draaiboek opzetten cybercrisisoefeningen
gebaseerd op cybercrisisoefening OZON

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

april 2017

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Inleiding

In oktober 2016 heeft SURFnet de grootschalige tweedaagse cybercrisisoefening OZON georganiseerd. In totaal oefenden 28 instellingen mee met in totaal ongeveer 200 deelnemers. Cybercrisisoefening OZON is een succesvolle eerste simulatieoefening geweest. De instellingen en spelers hebben actief en enthousiast geoefend. De oefening werd zeer goed beoordeeld, zowel op inhoud als op het behalen van oefendoelen.

Cybercrisisoefening OZON is een ‘gap bridging exercise geweest’ waarbij bruggen zijn geslagen tussen bestuurders, communicatie- en de ICT-afdelingen, zowel intern als tussen de instellingen. De verschillende lagen binnen de instellingen – bestuur, communicatie en ICT-afdelingen – hebben goed met elkaar gecommuniceerd. Dat was vaak voor het eerst met betrekking tot het onderwerp cybercrisis. Ook werd er veel tussen de instellingen overlegd. Het functioneren van de keten is getest en de effectiviteit van de crisiscommunicatie getoetst.

De deelnemers hebben het belang van oefenen voor het vergroten van het bewustzijn gevoeld. De spelers hebben het scenario als zeer realistisch, leuk en erg leerzaam ervaren. Sommige instellingen speelden ook na het signaal nog fanatiek door en de tweede dag werd opnieuw enthousiast gestart. Verschillende bestuurders vroegen of ze langer dan gepland mee mochten oefenen. Voor veel instellingen is OZON een directe aanleiding om meer aandacht aan cybersecurity te besteden.

De voorbereiding van de oefening was intensief en heeft veel tijd gekost. Ook voor de spelers bleek de oefening zwaarder dan verwacht. Dit was het echter gezien de impact waard. Cybersecurity staat op de kaart, kennis en bewustzijn zijn vergroot en er zijn bruggen geslagen tussen het tactisch/operationeel en strategisch niveau, zowel binnen als tussen instellingen.

Veel betrokkenen hebben de wens uitgesproken om vaker zowel grootschalige, als kleinschalige oefeningen te houden. Voor deze doelgroep hebben we deze handreiking gebaseerd op OZON opgesteld.

Deze handreiking en draaiboek cybercrisisoefeningen kan gebruikt worden voor het opzetten van zowel grootschalige als kleinschalige cyberoefeningen en is bedoeld voor (ICT- en) beveiligingsspecialisten. Deze oefeningen kunnen zowel binnen de instellingen als tussen instellingen of zelfs sectorbreed worden opgezet.

Leeswijzer
Hoofdstuk 2 gaat in op de planning van een cybercrisisoefening aan de hand van de stadia voorbereiding, de oefening en de evaluatie. Hoofdstuk 3 beschrijft de rollen, taken en acties en hoe die tijdens de voorbereiding en tijdens de oefening en evaluatie aan de orde komen. In hoofdstuk 4 worden de huishoudelijke taken, benodigdheden en materialen beschreven voor het opstellen van het scenario, de informatie voor de deelnemers en de benodigde documenten tijdens de oefening. Ook worden de verschillende middelen van communicatie besproken. Hoofdstuk 5 gaat in op de logistiek van de oefening. Hoofdstuk 6 zet uiteen hoe een (optionele) “Capture the Flag” oefening op te zetten is. Hoofdstuk 7 besteed aandacht aan de evaluatie, waarbij zowel de evaluatiemomenten als het evalueren van het oefenproces als het evalueren van de crisisstructuren besproken wordt.

Ten slotte vind je in de bijlagen een gedetailleerde uitwerking van een planning, checklist, verschillende vormen van oefeningen, voorbeelden van een scenario en andere informatie die behulpzaam is bij het opzetten en uitvoeren van een cybercrisisoefening.

Voor meer informatie over de achtergrond van risicomanagement en crisisbeheersing, de algemene achtergrond bij het opzetten van een cybercrisisoefening en de lessons learned uit cybercrisisoefening OZON verwijzen we naar de whitepaper over ‘cybercrisisoefening OZON, een gap bridging exercise’.

2. Planning cybercrisisoefening: voorbereiding, oefening en evaluatie

2.1. Uitgangspunten planning

Voor een simulatieoefening met de omvang van OZON is minimaal een half jaar voorbereidingstijd nodig. Hierbij dient rekening gehouden te worden met de voorbereidingstijd, vakanties, aantal vergaderingen, uitvoering en evaluatie.

De planning is afhankelijk van de complexiteit (operationeel/tactisch/strategisch), de omvang en de beschikbare middelen. Wanneer de oefening met meerdere instellingen tegelijk gespeeld wordt, moeten de instellingen zich aanmelden. Besluitvorming voor deelname op bestuurlijk niveau en grootschalige deelname kost tijd, zeker als ook het bestuurlijk niveau wordt aangehaakt. Houdt hier in de aanmeldprocedure rekening mee.

Bij OZON was aanvankelijk 27 april als deadline voor de aanmelding gesteld. Echter door het enorme enthousiasme hebben we de inschrijving vervroegd gesloten. Hierdoor konden verschillende deelnemers die nog geen besluit genomen hadden niet meer op het gewenste niveau meespelen. Eventueel bij een jaarlijks terugkerend evenement kan hier al in de jaarplanning rekening mee gehouden worden.

Wanneer men met veel instellingen samenspeelt is het nuttig om vergadermomenten van tevoren in te plannen. De meeste tijd wordt besteed aan het bedenken en uitwerken van het scenario.

In de planning wordt rekening gehouden met:
- datum en tijd van de oefening;
- duur van de oefening;
- beschikbaarheid sleutelspelers;
- andere evenementen om conflicten rondom beoogde uitvoeringsdatum zoveel mogelijk te voorkomen;
- besluitvormingsproces;
- vakantieperiodes;
- voorbereiding van het scenario;
- voorbereiding van het technische en strategische bewijsmateriaal voor het scenario;
- uitnodigen, informeren en brieven van deelnemers;
- evaluatie.

Zie [bijlage 5: planning tijdlijn OZON 2016] voor een grafische tijdlijn met data, deadlines, actiepunten, vergaderingen zoals gebruikt bij cybercrisisoefening OZON.

2.2. Tijdlijn/draaiboek organisatie cybercrisisoefening

Leg in een tijdlijn/draaiboek vast acties, activiteiten, deadlines en vergadermomenten vast. Leg ook vast wie waar verantwoordelijk voor is.

Taken waarbij rekening gehouden moet worden zijn:
- opdrachtgever vastleggen, budget en raakvlak creëren;
- projectgroep formeren;
- doelen, needs en nice to have list en oefenvorm bepalen;
- oefenlocatie vastleggen en logistiek zoals lunch regelen;
- vergaderingen projectgroep, programmagroep en stuurgroep plannen;
- naam bepalen;

- communicatiemedia bepalen en vastleggen;
- uitnodigen deelnemende instellingen;
- deadlines inschrijvingen;
- data en inhoud evaluatie(s) bepalen;
- schrijven scenario, zowel centraal als instellingsscenario's;
- bepalen of je een mediasimulator gebruikt en welke;
- communicatieplan bedenken en uitwerken;
- dagplanning oefendag/dagen maken voor oefening;
- dagplanning oefendag/dagen maken voor logistiek;
- draagvlak creëren binnen de instellingen;
- uitwerken documentatie voor de spelers;
- briefing spelers;
- technische elementen ontwerpen, uitwerken en uitrollen;
- interventies uitwerken;
- uitnodigen en informeren externe partijen eventueel om mee te spelen;
- evalueren en uitwerken van evaluatie;
- uitkomsten communiceren binnen de instelling(en);
- bronsoefening: infiltranten briefen en instrueren en verstrekken vrijwaringsbewijs.

Een voorbeeld van een draaiboek/tijdlijn van cybercrisisoefening OZON vind je in [bijlage 6: voorbeeld tijdlijn organisatie cybercrisisoefening OZON] en voor een checklist [bijlage 18: checklist opzetten crisisoefening]. Onderstaand worden de rollen en taken nader uitgelegd. Voorbeelden vind je in de bijlagen.

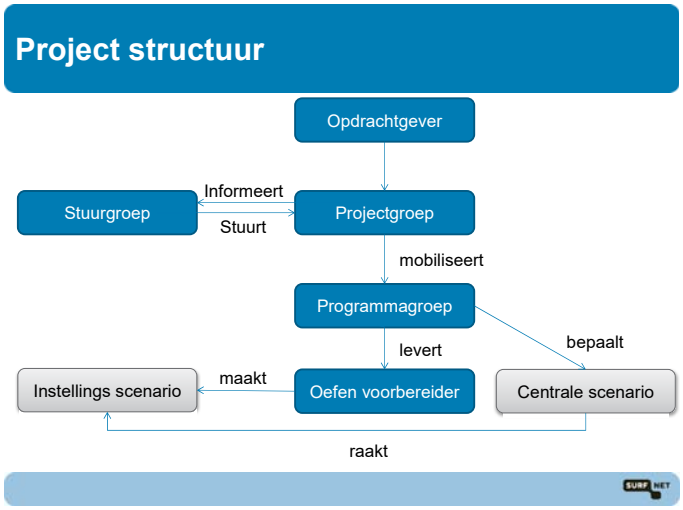
2.3. Randvoorwaarden

Houdt tijdens het opzetten van de oefening rekening met zaken zoals;
- impact op lopende processen en infrastructuur;
- de rol van de security officers;
- de rol van het voorbereidingsteam;
- voorwaarden om het spel te kunnen onderbreken;
- en ervoor te zorgen dat het spel gesloten blijft.

Zie voor een uitgebreide beschrijving [bijlage 4: randvoorwaarden voor het slagen van de oefening].

3. Rollen, taken en acties

3.1. Voorbereidend aan oefening



3.1.1. Opdrachtgever

De opdrachtgever stelt tijd, geld en mankracht beschikbaar om de crisisoefening uit te kunnen voeren.

3.1.2. Projectgroep

Stel een team samen met een projectleider, projectsecretaris, communicatiemedewerker, en projectleden.[1] Het projectteam is verantwoordelijk voor het scenario (zowel strategisch als technisch), de documentatie, de logistiek van de oefening en de evaluatie.[2] De deelonderwerpen kunnen door verschillende projectleden en/of binnen de projectgroep worden voorbereid.

De volgende rollen zijn in de projectgroep aanwezig, dezelfde persoon kan meerdere rollen vervullen.

- De **projectleider** is verantwoordelijk voor de planning en de uitvoering van de oefening. Bij een oefening van twee dagen dient voor de rol van projectleider ongeveer 15 dagen ingecalculeerd te worden.
- De **projectsecretaris** notuleert de vergaderingen, is verantwoordelijk voor het opzetten van een informatieplatform (bijvoorbeeld een wiki), en verstuurd alle centrale communicatie naar de stuurgroep, project- en programmagroep. Calculeer bij een oefening van twee dagen voor de projectsecretaris ongeveer 20 dagen in.
- De **communicatieadviseur** bedenkt en zet de interne en externe communicatiestrategie uit. Dit wordt eventueel in een communicatieplan vastgelegd. Voor de rol van communicatieadviseur dient voor een oefening van twee dagen ongeveer 5 dagen ingecalculeerd te worden. Zie [bijlage 13: Inhoud voor een communicatieplan].
- De **oefenleider** is tijdens het spel verantwoordelijk voor het verloop van de oefening en houdt contact met de projectleider en de centrale oefenstaf/responscel. De projectleider kan deze rol ook vervullen. Belangrijk is dat een oefenleider ervaring moet hebben met crisisoefeningen en moet kunnen improviseren. Calculeer voor de rol van oefenleider bij een oefening van twee dagen 5 dagen in. (Voorbereiden en begeleiden oefening).

---

[1] ISO 22398:2013(E), art. 5.2.4.1, p. 10
[2] ISO 22398:2013(E), art. 5.2.1, p. 8

- **Projectleden** nemen diversen (optionele) taken op zich:
    - **Technische voorbereiding van het scenario -** Voor de technische voorbereiding dient voor een oefening van twee dagen 24 dagen ingecalculeerd te worden. Zie [bijlage 10: technische elementen scenario].
    - **Uitwerken centraal scenario** - Hiervoor dient bij een oefening van twee dagen, 2 dagen ingecalculeerd te worden. Zie [bijlage 7: Opzetten scenario simulatieoefening].
    - **Begeleiding bij uitwerken instellingsscenario's** – Calculeer voor de begeleiding van de oefenvoorbereiders zonder ervaring, bij het maken van de instellingsscenario's, (bij 28 instellingen, waarvan 14 goud/zilver en 14 brons), voor een oefening van twee dagen 40 dagen in.
    - **Organisatie en adviestaken** hiervoor dient voor een oefening van twee dagen 45 dagen ingecalculeerd te worden. (Denk hierbij aan projectmanagement, stakeholdermanagement, verwerven middelen, faciliteren bijeenkomsten, vergaderingen en oefening, wiki opzetten en bijhouden, oefeningsdagen faciliteren, de leiding over de oefendagen, de logistiek en het opzetten, plannen en leiden van de (gezamenlijke) evaluatiesessies. Deze punten zullen verder in deze handreiking aan de orde komen.)
    - **Optioneel:** Het organiseren van **gezamenlijke werksessies/workshops** is een mogelijkheid om de expertise van het voorbereidingsteam te ontwikkelen. De oefenvoorbereiders kunnen gezamenlijk aan de scenario's werken, ervaringen uitwisselen en hun kennis verbreden. Hierdoor kan ook, indien dit een doel van de oefening is, de scenario's op elkaar worden afgestemd.

- **Optioneel: Externe partij –** Overweeg om externe expertise in te schakelen als er nog geen of weinig ervaring is met het opzetten van een cybercrisisoefening. Zet de externe expertise in bij de strategische invulling, bij het opzetten oefenmiddelen en als ondersteuning van de oefenleider.

Naam	Organisatie	Functie	Focus	Telefoonnummer
		Projectleider		
		Projectsecretaris		
		Communicatie		
		Projectlid		
		Projectlid		
		Oefenleider		

3.1.3. Optioneel: Programmagroep

Wanneer meerdere organisaties deelnemen aan de oefening is het raadzaam om naast het projectteam een programmagroep aan te stellen waarbij uit elke organisatie één lid als oefenvoorbereider deelneemt. Reken per oefenvoorbereider 5 dagen voorbereidingstijd voor een oefening van 5 dagen.

Voor een complexe oefening, waarbij meerdere partijen deelnemen, is het bovendien raadzaam om voor strategische beslissingen een overkoepelende stuurgroep aan te stellen. Stel in gezamenlijk overleg de oefendoelen vast [bijlage 1: oefendoelen vaststellen] en bepaal de oefenvorm [zie bijlage: 2 oefenvormen]. Zie hiervoor ook paragraaf 3.1.4 over de stuurgroep.

De projectgroep zorgt samen met de programmagroep dat het centrale scenario wordt vastgesteld en uitgewerkt. Verder hebben de programmagroepleden als taak:

- nemen deel aan de programma werkgroepen;
- lezen kritisch mee met het centrale scenario en beoordelen het centrale scenario;
- werken eigen instelllingsscenario uit.
- werken de master event list, en bijbehorende interventies uit en leveren details aan voor de generieke spelonderdelen;

- om de scenario's efficiënt uit te werken en daar waar nodig op elkaar te laten aansluiten kan dit met behulp van de projectgroep en door middel van samenwerkingssessies/workshops gedaan worden;
- briefen de spelers in de eigen achterban ter voorbereiding op de oefening op basis van de aangedragen informatieset;
- Geven invulling aan de simulatierol en leveren feedback aan spelers tijdens de oefening.

Naam	Instelling	Telefoonnummer

3.1.4. Optioneel: Stuurgroep

Voor een complexe oefening waarbij meerdere partijen deelnemen is het raadzaam om voor strategische beslissingen een overkoepelende stuurgroep aan te stellen. De stuurgroep bestaat uit leden van de deelnemende Goud instellingen en neemt beslissingen op strategisch niveau.

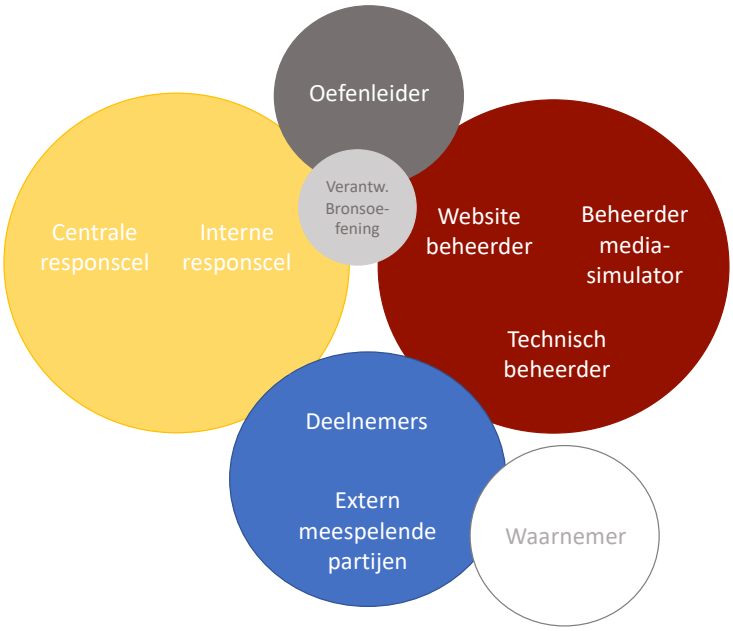
Naam	Instelling	Telefoonnummer

3.1.5. Deelnemende organisaties

- Bepaal of je alleen intern of met verschillende organisaties oefent.
- Indien je met meerdere organisaties oefent bepaal aan de hand van criteria zoals beschikbare voorbereidingstijd en capaciteit van ruimten hoeveel organisaties er mee kunnen doen.
- Bepaal op welke niveaus organisaties mee kunnen oefenen. Zie [bijlage 3: Rollen deelnemende instellingen].

3.2. Rollen en taken tijdens de oefening

Tijdens de oefening hebben projectgroep, deelnemers en waarnemer elk hun eigen rol. Hieronder tref je een overzicht van de rollen die ingezet kunnen worden om het spel in goede banen te leiden.



- De **oefenleider** houdt het centrale scenario in de gaten, overlegt met regelmaat met de responscellen om te inventariseren hoe de oefening bij de organisaties loopt en stuurt zo nodig bij. Dit kan door interventies toe te voegen of te verminderen of door alternatieven te bieden om het spel zo realistisch mogelijk te maken.
- De **centrale responscel** simuleert alle rollen van de buitenwereld zoals gemeentes of andere overheden, hulpdiensten zoals politie en brandweer, belangenverenigingen, journalisten e.d. en zet de algemene spelelementen uit.
- De **interne responscel** verspreidt de interventies voor de eigen organisatie en simuleert alle rollen van de interne betrokkenen die niet met de oefening meespelen en zet de instellingsspecifieke spelelementen uit.
- **Optioneel:** Tijdens de oefening kan een **waarnemer** aangewezen worden. De waarnemer kan op de werkvloer observeren of en hoe de gestelde doelen worden behaald. Deze waarnemingen kunnen een bijdrage leveren aan het evaluatieproces.[3] De waarnemer kan ook met de interne responscel schakelen om tijdens de oefening met interventies het scenario bij te sturen.
- **Optioneel: De beheerder mediasimulator** kan zorgen voor een goed gebruik van een gesloten systeem voor de mediaberichten en eventueel berichten toevoegen/corrigeren.
- **Optioneel: De website beheerder** beheert de eventueel gebruikte websites, en past ze waar nodig tijdens de oefening aan het spel aan.
- **Optioneel: De technisch beheerder** zorgt tijdens het spel dat eventuele problemen opgelost kunnen worden en aanpassingen aan malware e.d. gedaan kan worden.
- **Optioneel: Externe meespelende partijen** zijn partijen die in hun eigen rol mee-oefenen; bijvoorbeeld de AIVD, KLPD (Korps Landelijke Politie Diensten), NCSC (Nationaal Cyber Security Centrum) en AP (Autoriteit Persoonsgegevens)
- **Optioneel: verantwoordelijke voor de bronsoefening** die de communicatie met infiltranten en instellingen verzorgd over de Capture the Flag oefening, en vraagbaak is voor het ‘volgen van de simulatieoefening’.

[3] ISO 22398:2013(E), art. 5.4.2, p. 20

Partij	Betrokkenheid
Voorbeeld: KLPD	Voorbeeld: Oefenen mee in verband met het doen van aangiften
Voorbeeld: NCSC	Voorbeeld: Speelt eigen rol mee
Voorbeeld: AP	Voorbeeld: Oefenen aangiften datalek ‘simuleren middels geleverde informatie’

- De **deelnemers** zijn de spelers die op de werkvloer van de deelnemende organisatie(s) geconfronteerd worden met de acties en interventies. Zij moeten op basis van het crisisscenario acties en beslissingen nemen om de crisis te managen, alsof zij daadwerkelijk met een crisis te maken hebben.

Zie voor een overzicht van mogelijk deelnemende spelers en welke rollen door de responscellen tijdens een simulatieoefening gesimuleerd kunnen worden [bijlage 8: voorbeelden rollen interne spelers en gesimuleerde rollen door responscellen].

4. Huishoudelijke informatie, lijst van benodigdheden en materialen

4.1. Voorbereidend op de simulatieoefening

- **Centrale wiki –** om alle notulen, informatiedocumenten, bestanden e.d. te verzamelen en uit te wisselen. Maak eventueel speciale delen toegankelijk voor deelnemers, projectgroep, programmagroep en stuurgroep. Leg ook een **FAQ** aan met veelgestelde vragen.

4.1.1. Maken scenario

- Gebruik verschillende documenten als hulpmiddel bij het maken van het scenario. Deze dienen als format voor het scenario en geven een beeld van hoe het scenario te maken is.

  Voorbeelden van documenten zijn:
  - **vragenlijsten** om doelen en reikwijdte oefening bij de instellingen te bepalen;
  - document met informatie over **mogelijk gevoelige data** bij instellingen om de strategische scope te bepalen;
  - **voorbeeld master event list**, waarop eigen scenario elementen kunnen worden ingevuld;
  - **voorbeeld interventies** zoals krantenartikelen, blogs, e-mails, twitterberichten, vragen van Raad van Toezicht, vragen van juristen, etc.;
  - om begeleiding te geven bij het opstellen van het scenario kan een **aanvullende handleiding scenario's** verstrekt worden;
  - **geanonimiseerd voorbeeld instellingsscenario** – om als voorbeeld te dienen voor een eigen scenario;
  - Informatie voor de websites en de **malware en technische elementen;**
  - **handleiding** voor het aanleveren en installeren van de technische elementen.

4.1.2. Informatie voor deelnemers

- **E-mail richting organisatie -** uitleg over oefening
- **Voorbeeldpresentatie** - voor briefing spelers
- **E-mail uitnodiging spelers** voor de briefing
- **Informatiepakket voor de spelers** – bestaande uit:
  - begrippenlijst zie [bijlage 17: begrippen];
  - algemene informatie over de oefening;
  - spelregels zie [bijlage 11: spelregels spelers];
  - overzicht te ontvangen documenten zoals;
    - lead in;
    - teaser;
    - Adreslijst.

- **Lead in –** Je kunt voorafgaand aan de oefening, (eventueel dag van tevoren) een document verspreiden waarin de achtergrond bij het scenario en de huidige stand van zaken en beeld in de media en maatschappij wordt geschetst; zo starten alle deelnemers met dezelfde informatie.
- **Teasers –** Eventueel kunnen videofilmpjes of ander materiaal voorbereid en verspreid worden om de spelers op te warmen voor het spel.

4.2. Documenten tijdens oefening

- **Adreslijst –** Maak een adreslijst met alle deelnemers. Hiermee waarborg je een gesloten omgeving. Dit zorgt ervoor dat de oefening en realiteit zich niet gaan vermengen. Alleen de deelnemers

op deze lijst mogen worden benaderd. Als iemand niet op de adreslijst staat, dan nemen spelers contact op met de responscel

- De oefenvoorbereiders hebben het instellingsscenario uiteindelijk vastgelegd in een **'master event list'**, een combinatie van events voor het generieke scenario en instellingsspecifieke events.
- **De uitgewerkte 'interventies'**, zoals krantenartikelen, twitterberichten, social mediaberichten, blogs, e-mails etc. Evenals de interventies die via telefoon ingebeld zullen worden.

4.3. Communicatiemiddelen tijdens oefening

Om de communicatie gericht te laten verlopen, zowel tijdens de voorbereiding als tijdens de oefening zelf is het raadzaam om aparte mailadressen aan te maken. Bijvoorbeeld voor de projectgroep, programmagroep als de stuurgroep.
Het is nuttig om een mailadres aan te maken waar tijdens de oefening centraal op gelogd wordt. Zo kan alle communicatie in de gaten gehouden worden. Dit mailadres moet door de deelnemers in de cc van elke communicatie per mail gezet worden. Ook is het raadzaam om een mailadres aan te maken waar de oefenleiding tijdens de oefening op bereikbaar is, zodat deelnemers met vragen en opmerkingen direct de oefenleiding kunnen aanschrijven.
Niet elke instelling is aangesloten op de SCIRT- en SCIPR-maillijsten[4]. Het is daarom raadzaam om aparte maillijsten te maken voor alle instellingen die met de oefening meedoen. Zo mist niemand relevante informatie tijdens de oefening.

- Maak verschillende **e-mailadressen** aan voor tijdens de voorbereiding van de oefening en voor tijdens het spel:

Doelgroep	Mailadres
Projectgroep	
Programmagroep	
Stuurgroep	
Mailadres voor logging van e-mailverkeer	
Mailadres tijdens oefening voor alle spelcommunicatie	
Alternatief oefen-SCIPR-adres	
Alternatief oefen-SCIRT-adres	

- Maak ook **interne e-mailadressen** aan voor gebruik tijdens de oefening voor:

Doel	Mailadres
Mailadres waarnaar ge-cc'd wordt, zodat je alles in de gaten kunt houden	
Mailadres waar je als responscel op bereikbaar bent	

- Verder kan er gebruik gemaakt worden van communicatiemiddelen zoals **whatsapp, jabber, e.d.;** Bepaal ook welke andere communicatiemiddelen gebruikt worden.

[4] SCIRT en SCIPR zijn communities van ICT-experts van de op SURFnet aangesloten instellingen waar op operationeel en beleidsniveau kennis over security wordt uitgewisseld.

4.4. Mediasimulator

Gebruik een gesloten omgeving voor het verspreiden van berichten. Hiermee zorg je dat de oefening en de realiteit zich niet gaan vermengen. Hiervoor kan van een mediasimulator gebruik gemaakt worden. Een andere optie is om de mediaberichten via e-mail te verspreiden.
In een mediasimulator worden alle mediaberichten opgenomen; bijvoorbeeld facebook, twitter en krantenberichten. Berichten kunnen algemeen of instellingsspecifiek zijn. Toegang tot de mediasimulator is besloten en alleen voor de spelers om ongewenste spel inmenging te voorkomen. Tijdens het spel kunnen berichten worden toegevoegd en kan gereageerd worden op de social mediaberichten. Idealiter wordt de mediasimulator vooraf geprogrammeerd en speelt tijdens de oefening de berichten automatisch af. Middels de simulator kan zo nodig het spel vertraagd of versneld worden. Zo kan men in pas blijven lopen met de ontwikkelingen tijdens het spel en het tempo van de spelers.

- Bepaal of je gebruik maakt van een **simulatieomgeving** en van welke/of bouw hem zelf.

5. Logistiek van de simulatieoefening (goud- en zilverniveau)

5.1. Duur, data en locatie

Oefenduur - Bepaal hoeveel dagen de oefening mag duren en bepaald of er alleen binnen werktijden of ook in de avond of 24 uur doorgespeeld wordt.[5]
Oefendata - Kies een datum of meerdere data, houdt hierbij rekening met zaken zoals vakanties en ander evenementen.
Oefenlocatie - De locatie is afhankelijk van het soort oefening. Voor een simulatieoefening geldt:
- Spelers spelen op de eigen locatie in de eigen werkomgeving.
- De responscellen en oefenleiding bevinden zich op een centrale locatie van waaruit ze de oefening sturen.

5.2. Dagindeling simulatieoefening

Planning en dagindeling van de oefendagen
- Bereid de logistiek van de oefendagen voor.
- Maak een overzicht met het oefenprogramma.
  Zie [bijlage 14: voorbeeld oefenprogramma cybercrisisoefening].
- Stel voor de oefendagen een schema met planning en benodigdheden op.
  Zie [bijlage 15: voorbeeld schema oefendagen].

Denk hierbij ook aan catering en aan de tijd die nodig is voor vervoer, bijvoorbeeld om spelleiders op een centrale locatie te verzamelen.

Verloop van een simulatieoefening
- Bij een simulatieoefening oefenen spelers in hun eigen omgeving en wordt de oefening gestuurd vanaf een centrale locatie door de responscellen. Zie voor een voorbeeld van het verloop van een simulatieoefening [bijlage 9: verloop van een simulatieoefening].

5.3. Briefing deelnemers, organisatie en responscel

- Houdt voorafgaand aan de oefening een **briefing met de deelnemers** om de uitleg over de oefening te geven. Bespreek de oefendoelen, de spelregels en de wederzijdse verwachtingen.
- Kies of je van tevoren de organisatie inlicht over de oefening en in welke mate van detail je dat wil doen.
- Bespreek kort voorafgaand aan de oefening met de responscel de oefendoelen, verwachtingen en details. Zie voor een uitgebreide beschrijving [bijlage 12: briefing deelnemers, organisatie en responscel].

[5] Vanwege logistieke redenen en omdat het de eerste keer was is OZON alleen tijdens werktijden gespeeld

6. Optioneel: Observatie en Capture the Flag oefening (Brons)

6.1. Voorbereidend op de bronsoefening

Bij OZON observeerden bronsdeelnemers de oefening en kregen een ‘Capture the Flag’ opdracht.

Observatie
Deelnemers krijgen enkele dagen van tevoren inloggegevens om tijdens de simulatieoefening via de mediasimulatieomgeving de crisis te kunnen volgen. Indien mediaberichten via de e-mail verspreid worden kunnen deze berichten ook naar de bronsdeelnemers gestuurd worden.

Capture the Flag
Er kan gekozen worden om naast het observeren van de crisisoefening ook een spelelement toe te voegen. Tijdens OZON bleek het lastig om meerdere oefensystemen tegelijk te besturen. Dit element kan ook apart gespeeld worden.

- Regel studenten of vrijwilligers als infiltrant om de ‘Capture the Flag’ opdracht uit te voeren.
- Maak ‘aanvalssoftware’ die door de instellingen opgespoord moet worden.
- Instrueer de infiltranten over het gebruik van een laptop en gebruik van de malware.
- Voorkom dat er daadwerkelijk schade aangericht wordt, voeg geen extra, voor de oefening overbodige, functionaliteit toe aan de malware en instrueer de infiltranten zich aan de regels te houden
- Plan een testmoment met de infiltranten om te kijken of alles werkt.
- Verstrek aan infiltranten een vrijwaringsbewijs om duidelijk te maken dat zij in opdracht van instelling(en) aanwezig zijn en de software op hun laptop draaien.
- Stel een oefenvoorbereider bij de instelling op de hoogte, deze kan intern de oefening sturen.

6.2. Dagindeling bronsoefening

Observatie
- Deelnemers kunnen inloggen op de mediasimulatieomgeving en gedurende de dag de berichten volgen. Indien mediaberichten via de e-mail verspreid worden, krijgen zij dezelfde berichten als de goud- en zilverspelers maar hoeven zij er niet op te acteren.

Capture the Flag
- Infiltranten bewegen zich in de ochtend door de gebouwen van de bronsinstelling. Hierdoor kunnen zij niet direct vonden worden. Naarmate de dag vordert kunnen ze een vaste plek innemen zodat ze makkelijker te vinden zijn. Ze hebben een laptop met simulatiemalware bij zich.
- Er kunnen interventies uitgezet worden om de instellingen op het juiste spoor te zetten.
- Aan het einde van de dag/oefening wordt duidelijk gemaakt middels berichtgeving welke bedreiging aanwezig was en hoe ze deze hadden kunnen vinden als dat nog niet gebeurd is. Ook worden de logbestanden vrijgegeven zodat er nader onderzoek kan plaatsvinden.

7. Evaluatie

Gestructureerde monitoring en evaluatie helpen om de feedback en de geleerde lessen in de organisatie te kunnen toepassen. Maak voor het evalueren gebruik van de ervaringen van deelnemers, het voorbereidingsteam en de waarnemers. Spreek deze ervaringen gezamenlijk door in evaluatiesessies. Ook kun je een online survey inzetten om de mening van de projectgroep, de programmagroep en de deelnemers te inventariseren.

7.1.1. Evaluatiemomenten

Plan verschillende momenten van evaluatie:

- **Hot wash/tijdens het spel -** Tijdens het spel kan aan spelers een checklist/vragenlijst gegeven worden om hun bevindingen meteen te monitoren. Dit kan de basis zijn voor latere evaluatiemomenten, zo blijven belangrijke evaluatiepunten top of mind. Spelers kunnen zowel punten noteren over de oefening als punten over de interne processen. Ook kan al tijdens de oefening in deelgroepen of aan het einde van de eerste dag gezamenlijk geëvalueerd worden en tussenresultaten besproken worden.
- **Direct na het spel -** organiseer direct na het spel een evaluatiemiddag. Als je binnen één instelling speelt dan kun je zowel conclusies over het verloop van de oefening als de interne processen bespreken. Als je met meerdere organisaties speelt is het goed om te bepalen of je alleen de oefening evalueert of ook de interne processen van de organisaties. Omdat inhoudelijke processen gevoelig kunnen liggen, kan het en overweging zijn om deze slechts intern te evalueren en niet in een groep.
- **Een aantal weken na het spel** - met de oefenleiding (projectgroep, programmagroep en stuurgroep) om het verloop en de resultaten van de oefening te bespreken.
- **Een aantal weken na het spel -** in de interne organisatie van de speler de bevindingen van alle teams op een rij zetten en algemene conclusies en bevindingen beschrijven.

7.1.2. Niveaus

Er zijn verschillende niveaus waarop de uitkomsten van de oefening geëvalueerd kunnen worden.

- **Oefenproces** - Kijk of het proces van de oefening goed is verlopen. De focus ligt hierbij op de organisatie van de oefening en hoe de oefening door het voorbereidende team en door de deelnemers is ervaren.
- **Interne crisisstructuur** - Evalueer of en hoe de crisisstructuur binnen de organisatie tijdens de oefening heeft gefunctioneerd. Dit kan op overkoepelend niveau met alle deelnemers/instellingen en/of binnen de instelling zelf.
- **Kennisdeling tussen organisaties** - Indien meerdere instellingen deelnemen: evalueer of/en hoe onderling is samengewerkt en kennis is gedeeld.

7.1.3. Interne waarnemer

- De waarnemer observeert op de werkvloer of en hoe de gestelde doelen worden behaald. Deze waarnemingen leveren een bijdrage aan het evaluatieproces. De waarnemer schakelt ook met de interne responscel om het scenario tijdens de oefening met interventies bij te sturen.

7.2. Data, locatie, vorm

- Plan op welk moment je wilt evalueren.
- Plan wat je wilt evalueren.
- Kies vorm van evaluatie. (Bijvoorbeeld een meeting, survey, per team, met complete groep deelnemers).
- Kies locatie voor de evaluatie en bepaal de genodigden.

7.3. Survey

Direct na de oefening kunnen online vragenlijsten naar de deelnemers gezonden worden met vragen over het oefenproces en/of vragen over het behalen van de (interne) oefendoelen, eigen bevindingen, succes- en leerpunten.

- Stel vragen voor de survey op
- Lanceer de survey na de oefening
- Verwerk de uitkomsten van de survey in de totale evaluatie

Zie voor de achtergrond [bijlage 16: evaluatie.]

Bijlage 1: Oefendoelen vaststellen

Hoofd- en sub-oefendoelen

Het centrale oefendoel van cybercrisisoefening OZON is;
- de weerbaarheid en awareness van instellingen in een cybercrisissituatie vergroten.

De sub-oefendoelen zijn:
- het functioneren van de interne en externe keten testen;
- de effectiviteit van de crisiscommunicatie toetsen;
- samenwerking tussen en binnen de instellingen vergroten.

Interne oefendoelen

Op basis van de hoofd- en subdoelen van de oefening hebben instellingen interne doelstellingen geformuleerd.

De meest voorkomende interne doelen zijn:
- het stimuleren van security awareness;
- het bewust worden van cyberrisico's;
- het testen van de interne en externe communicatie;
- het testen van tijdige evaluatie;
- het verbeteren van de communicatie tussen operationeel- en managementniveau;
- het testen of de interne processen goed ingericht zijn bij een cybercrisis;
- het testen van de securityprotocollen.

Andere doelen kunnen zijn:
- het testen van samenwerking met externe partijen;
- het testen van samenwerking in de keten.

Bijlage 2: Oefenvormen

In dit draaiboek is een grote cybercrisiscommunicatieoefening beschreven. Er zijn verschillende soorten oefeningen met verschillende intensiteit en omvang mogelijk. Hieronder tref je een overzicht aan van mogelijke oefenvarianten.

Crisisoefeningen kunnen in twee typen worden ingedeeld:

1. **Discussie-oefeningen**[6] waarbij deelnemers vertrouwd raken met de plannen, het beleid en de procedures. Bij discussie-oefeningen wordt een specifiek dilemma voorgelegd waar deelnemers in een vooraf gedefinieerde vorm over discussiëren.

2. **Praktijkoefeningen** worden gebruikt om plannen, beleid en procedures te testen en medewerkers te trainen. Meestal kiest men voor een vorm van simulatie die aansluit op een realistische omgeving.

Voorbeelden van discussie-oefeningen

- **Desk Check** - Een desk check is een methode om (wijzigingen van) plannen en procedures te valideren. Meestal gebeurt dit in een gesprek met de auteur van de plannen en procedures. In dit gesprek worden de plannen en procedures aan de hand van een scenario stap voor stap doorlopen. Dit maakt duidelijk welke stappen nodig zijn en hoe deze uitgevoerd moeten worden.

- **Walkthrough** - Een walkthrough geeft de mogelijkheid om een specifiek scenario, bijvoorbeeld een cybercrisis, uit te diepen. Een walkthrough laat zien wie wat wanneer doet en wat voor maatregelen je kunt nemen. Met een walkthrough kan heel specifiek de verschillende stappen in een crisis doorlopen worden, van detectie tot opschaling, respons, nabehandeling en afsluiting van de situatie. Een walkthrough duurt gemiddeld een dagdeel. Een walkthrough kan zowel intern geoefend worden als met andere partners die een rol tijdens een crisis spelen.

- **Workshop** - In een workshop kan naast het stap voor stap doorlopen van een scenario ook de reacties en acties van deelnemers besproken worden. Het is mogelijk om de reacties en acties van teams en individuele deelnemers te repeteren zonder tijdsdruk. Dit helpt om goed met crisissituaties en scenario's om te gaan.

- **Tabletop-oefening** - Bij een tabletop-oefening worden aspecten van het crisismanagement doorlopen. Spelers krijgen van tevoren dezelfde informatie over de gesimuleerde crisissituatie en over hun rol. Tijdens de oefening kunnen spelers gebruik maken van gesimuleerde (media)berichten. Het crisisteam kan met de tabletop relevante informatie delen, overzicht krijgen en (adequate) besluiten en (communicatie)maatregelen nemen.[7] Een tabletop is een goede optie als men in relatieve rust de crisisstructuur en de onderlinge samenwerking wilt oefenen en/of specifieke vaardigheden wilt trainen. Ook wanneer een organisatie (nog) niet toe is aan een interactieve simulatieoefening is een tabletop-oefening een goede optie.

Voorbeelden van praktijkoefeningen

- **Comms check** - Een Comms check voer je uit om communicatiemethoden en kennisgevingssystemen te checken en valideren. Deze oefenvorm wordt gebruikt om de systemen en infrastructuur te checken en te testen of alles werkt.

---

6 ISO 22398:2013 benoemt ze ook wel als "dilemma exercises"; art. 5.2.13, p. 16
7 http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ (geraadpleegd op 05 september 2016)

- **Oproepoefening** - Hierbij test je of je binnen de afgesproken tijd een crisisteam bij elkaar krijgt.

- **Distributed tabletop-oefening** - Bij de distributed tabletop-oefening worden plannen en procedures doorlopen op basis van een scenario waarbij spelers hun rol volgens routine spelen. Deze oefening is qua opzet gelijk aan een tabletop-oefening, maar er is geen mogelijkheid tot discussie. Deelnemers moeten handelen alsof er daadwerkelijk een crisis plaatsvindt. De mogelijke reacties kunnen eventueel later in een evaluatie worden besproken. Dit heeft als voordeel dat deelnemers de handelingen routinematig kunnen oefenen.

- **Een Command Post Exercise (CPX) -** Bij een CPX (zandbakoefening) wordt een crisis gesimuleerd zonder inzet van hulpdiensten, externe omgevingsfactoren en spelers. De crisisteams krijgen in een realistisch en evoluerend scenario vragen en opdrachten. Zo kunnen de teams in hun eigen omgeving met hun eigen faciliteiten, acties en reacties op een veranderend scenario oefenen.

- **Simulatieoefening** - Bij een simulatie speelt men in de eigen omgeving een realistisch scenario na. Deelnemers oefenen zoveel mogelijk onder normale omstandigheden met eigen middelen in de eigen omgeving. Het scenario van de oefening ontwikkelt zich aan de hand van de eigen besluiten en acties. Een simulatieoefening is geschikt als men wil oefenen onder druk en de reacties van deelnemers in de eigen omgeving wil testen en trainen. De intensiteit en de ontwikkeling in het scenario hangen af van het aantal deelnemers en hun ervaringsniveau. Ook is het van belang of alleen interne of ook externe partijen deelnemen. Een simulatieoefening duurt een dagdeel tot meerdere dagen.

- **Capture the Flag** - Bij een operationele Capture the Flag is het de bedoeling om een ‘vlag’ of ander element te vinden en veroveren. Dit kan in teams of individueel en wel of niet in competitieverband. Bij een cybergerelateerde Capture the Flag is vaak het doel om hackers in (gesimuleerde) ICT-systemen op te sporen en te pakken te krijgen.

- **Red Team/ Blue Team -** Bij een Red Team/Blue teamoefening valt het rode team het netwerk of een ander belangrijk bedrijfsonderdeel aan en moet het blauwe team de aanval proberen te verijdelen. Deze oefening vergroot het bewustzijn van mogelijke risico’s. Ook geeft de oefening inzicht in de mogelijke kwetsbaarheden en de methoden om hiermee om te gaan. Bovendien geeft de oefening inzicht in strategieën om een aanval te detecteren en erop te reageren.

Laagdrempelige voorbeelden voor oefeningen zijn bijvoorbeeld te vinden op Linux journal.[8]

[8] https://www.linuxjournal.com/content/example-security-exercises (geraadpleegd op 21 december 2016)

Bijlage 3: Rollen deelnemende instellingen

Niveau	Inhoud
Goud	De instelling levert minstens 5 mensen die meespelen. Op dit niveau spelen medewerkers mee die strategische beslissingen nemen, zoals leden van het College van Bestuur.
Zilver	De instelling levert minimaal 3 mensen uit de organisatie. Het is niet noodzakelijk om mensen uit het strategisch crisisteam te leveren, er wordt vooral op operationeel niveau geoefend.
Brons	Instellingen hebben vooral een observerende rol. Zij observeren hoe de oefening verloopt en kijken met het spelverloop mee. Je kan kiezen om een ‘Capture the Flag’ oefening of iets vergelijkbaars toe te voegen.

Bijlage 4: Randvoorwaarden voor het slagen van de oefening

- **De duur van de oefening** is afhankelijk van de oefendoelen, beschikbaarheid van de deelnemers en de impact op de organisatie (vakanties e.d.). De duur van de oefening kan variëren van een paar uur tot een paar dagen. Ook zijn oefenvormen mogelijk die enkele weken duren. Dit zal dan niet een fulltime oefening zijn, maar uit opdrachten naast de bestaande werkzaamheden bestaan.

- **Impact op lopende processen:** Je kunt kiezen om de dagelijkse bedrijfsvoering niet te veel te verstoren en de **impact op de lopende processen** binnen de organisatie zo minimaal mogelijk te zijn.

- **Impact op infrastructuur:** Om geen impact te hebben op de bestaande infrastructuur kan gebruik gemaakt worden van een simulatieomgeving van de bestaande productieomgeving. Deze kun je (laten) bouwen. Ook kun je voor technische impact gebruik maken van bijvoorbeeld; simulatiemalware en raspberry pi's. De instellingen kunnen zelf kiezen of ze hier gebruik van maken.

- **Rol van security officers:** Wanneer veel security officers deel uitmaken van het voorbereidingsteam als oefenvoorbereider, zijn zij niet aanwezig op de eigen locatie. Bij OZON hebben instellingen hiervoor zelf een passende oplossing gevonden. Dit biedt de kans om te oefenen hoe de organisatie functioneert bij afwezigheid van de security officer.

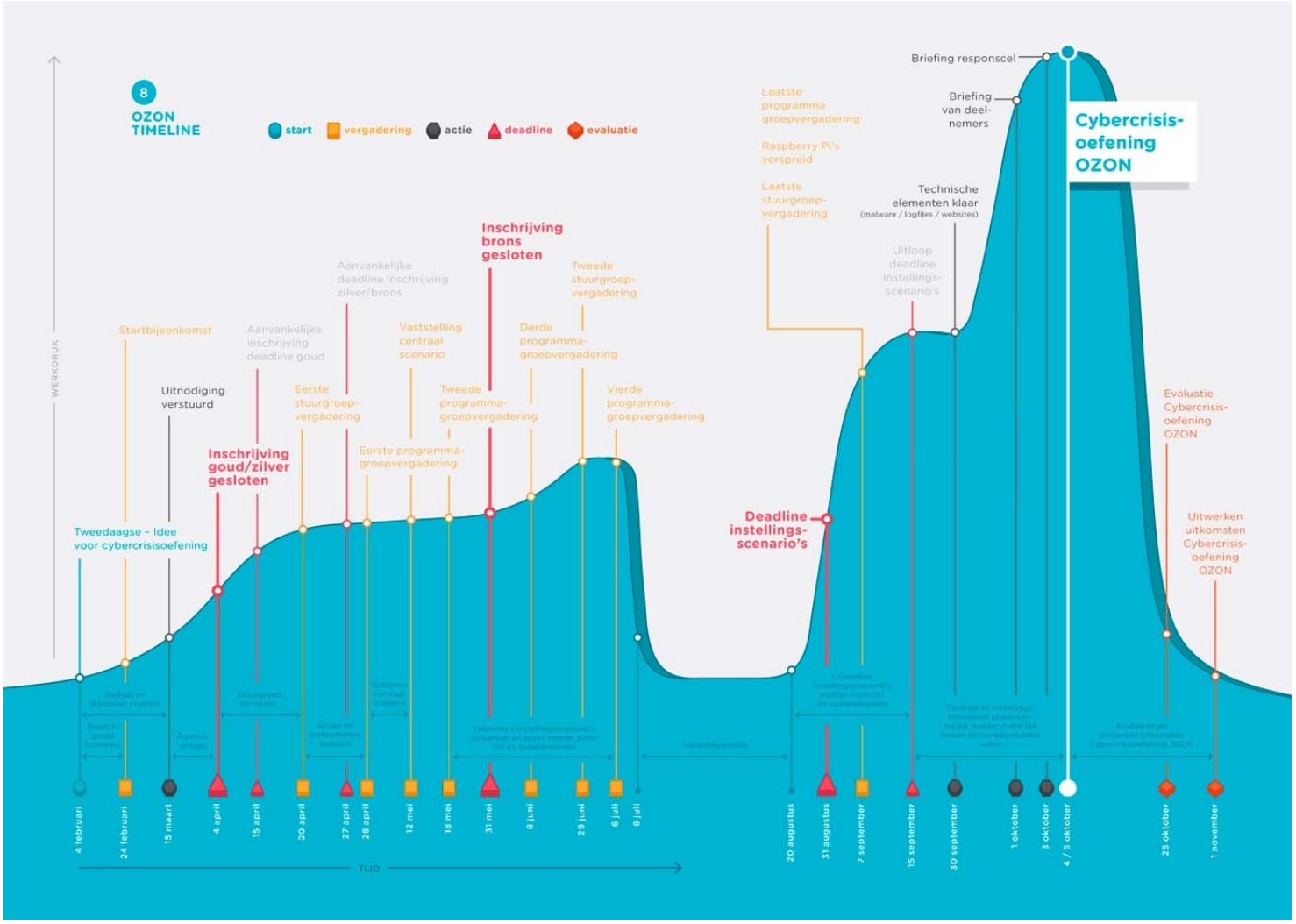
- **Oefenvoorbereiders:** Om het scenario te ontwerpen is specifieke kennis van de organisatie nodig. Bepaal daarom van tevoren wie deze kennis in huis heeft, wie als oefenvoorbereider de oefening voorbereidt en wie bij de instelling meedenkt over het mogelijke instellingsscenario. De oefenvoorbereiders kunnen niet deelnemen aan de oefening zelf. Houdt hier rekening mee.

- **No Play-situatie:** Er kunnen onvoorziene situaties optreden tijdens de oefening die niet rechtvaardigen om door te spelen. In dat geval zal de oefening gestaakt worden. De bevoegdheid om de oefening stil te leggen (No Play-situatie) ligt bij de projectleider.

- **Waarborgen gesloten karakter:** Om te voorkomen dat een oefenscenario als een echte crisis wordt opgevat, moet men maatregelen nemen die een **gesloten karakter** waarborgen. De oefenleiding stelt hiervoor spelregels op. Een 'gesloten' adreslijst met deelnemers en een gesloten omgeving voor het verspreiden van berichten zorgen ervoor dat de oefening en realiteit zich niet gaan vermengen. Alleen de deelnemers op deze lijst mogen worden benaderd. Als iemand niet op de adreslijst staat wordt contact opgenomen met de responscel.

Bijlage 5: Planning tijdlijn OZON 2016

In onderstaand figuur vind je een visuele weergave van de tijdlijn met data, deadlines en actiepunten van de organisatie, uitvoering en evaluatie van een cybercrisisoefening. Deze tijdlijn is een weergave van de planning en organisatie welke gebruikt is bij cybercrisisoefening OZON 2016. Een uitgebreide uitwerking van een tijdlijn/draaiboek met taken/data en verantwoordelijkheden vind je in [bijlage 6: tijdlijn organisatie cybercrisisoefening OZON].



Bijlage 6: Tijdlijn organisatie cybercrisisoefening OZON

Onderstaande tijdlijn is een voorbeeld van de planning van cybercrisisoefening OZON. In de handreiking met bijlagen worden de verschillende activiteiten nader uitgelegd.

Categorie	Datum	Activiteit	Verantwoordelijke
START	**4/5 feb**	**Start opzetten cybercrisisoefening**	
Activiteit	Tussen 4/5 feb en 24 feb	Opdrachtgever vastleggen; Projectgroep formeren.	
Activiteit	Tussen 4/5 feb en 24 feb	Hoofddoel oefening bepalen; Oefenvorm bepalen; Oefenduur, oefendata en oefenlocaties bepalen.	
Activiteit	Tussen 4/5 feb en 15 maart	Budget en draagvlak creëren.	
Activiteit	Tussen 24 feb en 15 maart	Locaties reserveren, en faciliteiten voor de oefening zoals lunch plannen en vastleggen. Zie voor details ook de bijlage schema oefendagen.	
Vergadering	24 februari	Startbijeenkomst	
Activiteit	24 februari	Naam van de oefening bepalen.	
Activiteit	24 februari	Centrale wiki in de lucht.	
Activiteit	15 maart	Uitnodigingen deelnemers versturen.	
Activiteit	Tussen 15 maart en 27 april	Tijd voor aanmeldingen deelnemers.	
Deadline	**4 april**	**Bij OZON is de inschrijving voor Goud/Zilver eerder gesloten in verband met groot aantal aanmeldingen.**	
Activiteit	Tussen 4 april en 20 april	Stuurgroep met goudleden formeren.	
Vergadering	20 april	Eerste stuurgroepvergadering.	
	20 april	Need/nice to have list bepalen met stuurgroep.	
Activiteit	20 april	Oefenvoorwaarden voor de oefeningbepalen.	
Deadline	**27 april**	**Officiële deadline aanmeldingen Goud/Zilver**	
Vergadering	28 april	Eerste programmagroepvergadering	
	28 april	Data en inhoud van de evaluaties bepalen.	
Activiteit	28 april	Scope/ oefendoelen meespelende instellingen bepalen. Need/nice to have list bepalen.	

Activiteit	Tussen 28 april en 12 mei	Schrijven centraal scenario.	
Activiteit	Tussen 28 april en 18 mei	Bepaal of je een mediasimulator gebruikt; welke en/of zelf bouwen.	
Activiteit	Tussen 28april en 18mei/ aanscherping voor 15 sept.	Communicatiestrategie en plan uitwerken.	
Vergadering	12 mei	Vaststelling centraal scenario.	
Vergadering	18 mei	Tweede programmagroepvergadering.	
Activiteit	Tussen 12 mei en 8 juli	Globale dagplanning oefendagen maken. Zie [bijlage 15: schema oefendagen].	
Activiteit	Tussen 12 mei en 5 september	Uitnodigen externe partijen zoals politie, NCSC etc.	
Activiteit	Tussen 12 mei en 15 september	Uitwerken en bespreken documentatie - Lead in - Informatiepakket spelers - E-mail richting organisatie - Materiaal voor briefing spelers - E-mailuitnodiging spelers briefing - Adreslijst - Eventueel teasers	
Activiteit	Tussen 12 mei en 15 september	Draagvlak creëren bij de spelers binnen de instellingen.	
Activiteit	Tussen 12 mei en 15 september	Bepaal of je een waarnemer inzet voor interne waarneming en zo ja; regel waarnemers.	
Activiteit	Tussen 18 mei en 8 juli	Dilemma's instellingsscenario's en opzet master event list uitwerken, spelelementen en technische elementen uitwerken.	
Deadline	**31 mei**	**Inschrijving Brons gesloten**	
Vergadering	8 juni	Derde programmagroepvergadering.	
Vergadering	29 juni	Tweede stuurgroepvergadering.	
Vergadering	6 juli	Vierde programmagroepvergadering.	
Vakantie	8 juli tot 20 augustus	Vakantieperiode	
Activiteit	Tussen 20 augustus en 31 september	Uitwerken instellingsscenario's master event list, spelelementen en technische elementen	
Deadline	**31 augustus**	**Deadline instellingsscenario's**	
Activiteit	Tussen 1 september en 15 september	Toetsen niveau en inhoud instellingsscenario's.	
Vergadering	7 september	Laatste programmagroepvergadering	

Activiteit	7 september	Raspberry Pi's verspreiden.	
Vergadering	7 september	Laatste stuurgroepvergadering	
Uitloop Deadline	**15 september**	**Uitloop deadline instellingsscenario's**	
Deadline	15 september	Documentatie af.	
Activiteit	15 september	Oefencommunicatiemiddelen voor tijdens de oefening – in de lucht.	
Activiteit	Tussen 15 september en 4 oktober	Centrale en instellingsspecifieke elementen uitwerken. (Zowel technisch als strategisch.) Totale master event list maken. Mediasimulator vullen met interventies.	
Activiteit	Tussen 15 september en 4 oktober	E-mail naar deelnemers versturen voor uitnodiging voor briefing.	
Activiteit	Tussen 15 september en 4 oktober	Briefen spelers en organisatie.	
Activiteit	Tussen 15 september en 4 oktober	E-mail naar organisatie versturen over oefening.	
Activiteit	30 september	Technische elementen klaar (malware/logfiles/websites/simulatie-Omgeving/aanvalssoftware voor de brons oefening)	
Activiteit	30 september	Infiltranten briefen over bronsoefening en vrijwaringsbewijs versturen naar infiltranten.	
Activiteit	30 september	Briefing van deelnemers	
Activiteit	03 oktober	Briefing responscel	
OEFENING	**4/5 oktober**	**Cybercrisisoefening OZON**	
Evaluatie	5 oktober	Hot wash evaluatie cybercrisisoefening OZON	
Evaluatie	**25 oktober**	**Evaluatie cybercrisisoefening OZON** met project-, programma en stuurgroep	
Activiteit	Tussen 5 oktober en 01 november	Evalueren en uitwerken uitkomsten cybercrisisoefening OZON.	

Zie voor een checklist gebaseerd op bovenstaande genoemde deadlines [Bijlage 18: checklist opzetten (cyber)crisisoefening Model OZON].

Bijlage 7: Scenario simulatieoefening

Centraal scenario

Op basis van vooraf opgestelde oefendoelen ontwerp je een scenario dat voldoende aanknopingspunten biedt voor de instellingen. Zie [bijlage 1: oefendoelen vaststellen]. Elke afdeling en/of instelling kan hier zijn eigen scenario op aanhaken. Ontwerp het scenario zo dat het als kapstok dient voor de instellingsscenario's van zowel de goud- als zilverspelers. Deze scenario's zijn de basis van de cybercrisisoefening.

Creëer een situatie waarbij opgeschaald en geëscaleerd moet worden om het scenario voor de Goud spelers, waarbij onder meer het College van Bestuur meespeelt, aantrekkelijk te maken. Houdt hierbij rekening met de beschikbaarheid van het College van Bestuur en leg vast of ze op een vast tijdstip aanhaken of gedurende het gehele spel meespelen.
Zorg dat het scenario de mogelijkheid biedt om op sommige afdelingen/instellingen een zwaardere impact te hebben dan op anderen. Zo kan het scenario naar wens worden aangepast.

Uitgangspunten scenario

Stel voorafgaand aan het schrijven van het scenario met de programmagroep/stuurgroep een '**need/nice to have list'** op die de voorwaarden scheppen voor het scenario.

Enkele voorbeelden van voorwaarden voor het scenario kunnen zijn:
- de deelnemers kunnen zowel de interne communicatie als de escalatie naar strategisch niveau oefenen;
- de oefening dient zowel voor crisismanagement als voor IT-afdelingen voldoende uitdaging te bieden;
- het scenario dienen voor alle verschillende instellingen die meespelen dienen voldoende herkenbare en realistische elementen bevatten;
- het scenario moet voldoende lastige dilemma's bevatten om te zien of deelnemers op tijd knopen doorhakken
- om te zorgen dat de crisis niet op te lossen is zonder te schakelen met het strategisch niveau kunnen zowel technische als strategische dilemma's aan de orde komen die de deelnemers niet zonder een strategische beslissing kunnen oplossen;
- om ervoor te zorgen dat instellingen met elkaar moeten afstemmen kan het spel voorzien worden van een ethisch element.

Voorbeelden van dilemma's die de aandacht van het college van bestuur vereisen zijn:
- imagoschade;
- claims;
- persoonlijke reputatie;
- reputatie organisatie;
- bestuurlijke aansprakelijkheid;
- ethische kwesties.

Deze dilemma's zouden de volgende risico's met zich mee kunnen brengen:

- openbaarmaking van:
  - medische dossiers;
  - persoonsgegevens;
  - onderzoeksdata;
  - bedrijfsgegevens;
  - organisatiegegevens;
- afpersing;
- geëncrypte databestanden;

- spionage;
- aangepaste/gemanipuleerde gegevens.

Centraal Scenario (Voorbeeld scenario)
Het centrale scenario van OZON bestond uit twee simultane dreigingen: een aanval van een idealistisch hackerscollectief en een criminele component.

Op basis van bovenstaande uitgangspunten is bij OZON gekozen om een deel van de oefening vanuit een fictief idealistisch hackerscollectief te laten komen, dat door een groot deel van Nederland (en binnen de instellingen) als sympathiek wordt gezien. Dit collectief heeft zowel een ethische als een criminele component. Hierdoor zijn de dilemma's niet zomaar van tafel te vegen. De dreiging van deze hackers raakt de gehele onderwijs- en onderzoekssector. Dit stimuleert de samenwerking tussen de instellingen.

Het hackerscollectief vindt dat er te veel informatie in bezit is van bedrijven en instanties die om economische redenen niet publiek gemaakt wordt. Hun visie is dat de ontwikkeling van de menselijke beschaving versneld wordt als alle data beschikbaar is voor iedereen. Het niet delen van informatie hindert vooruitgang en daarom zijn ze fel tegen alle vormen van intellectueel eigendom. Hun doel is om zoveel mogelijk gegevens integraal openbaar te maken. Hierbij houden ze geen rekening met privacygevoelige data.

Het hackerscollectief heeft in de publieke opinie veel credits verdiend met hun onthullingen en heeft nu aangekondigd de activiteiten uit te breiden naar Nederland. Hierbij hebben zij de pijlen ook op de onderwijs- en onderzoekssector gericht. Het scenario heeft een sterk technische component om hun doel te bereiken. Ze hebben op grote schaal malware verspreid. Het is multifunctionele malware die bestanden kan verzamelen en doorsturen, maar ook in staat is om op commando alle bestanden op de computer of aangesloten netwerk te versleutelen. Hiermee heeft het hackerscollectief veel gevoelige data verzameld. In een media-offensief zal het hackerscollectief deze data openbaar maken.

Aan medewerkers van Nederlandse onderwijs- en onderzoeksinstellingen wordt door het collectief gevraagd de malware executable te downloaden en installeren op instellingscomputers. De executable verspreidt zichzelf via een Windows zero-day en maakt zo nieuwe datacollectie mogelijk. Bovendien wordt gevraagd om een mirror te maken van de website met onthulde data. Er is onder andere van raspberry pi's gebruik gemaakt om deze mirrors in de lucht te brengen.

Een aantal hoogleraren heeft aanvankelijk steun uitgesproken aan het onthullen van de data. Ze veroordelen weliswaar het hacken, maar steunen de onthullingen omdat deze ethisch onverantwoord onderzoek aankaarten. Ook wordt een webpetitie gestart, die onderzoekers kunnen ondertekenen.

Daarnaast kent het scenario een criminele component. Een journalist ontdekt een webportal waar het mogelijk is om cijfers tegen betaling aan te passen, cijferadministraties openbaar te maken, medische dossiers van bekende Nederlanders openbaar te maken, compromitterende foto's van medestudenten en docenten te openbaren en tentamengegevens in te zien. Een mogelijke link met het hackerscollectief wordt gesuggereerd, maar het is niet duidelijk of deze er ook echt is.

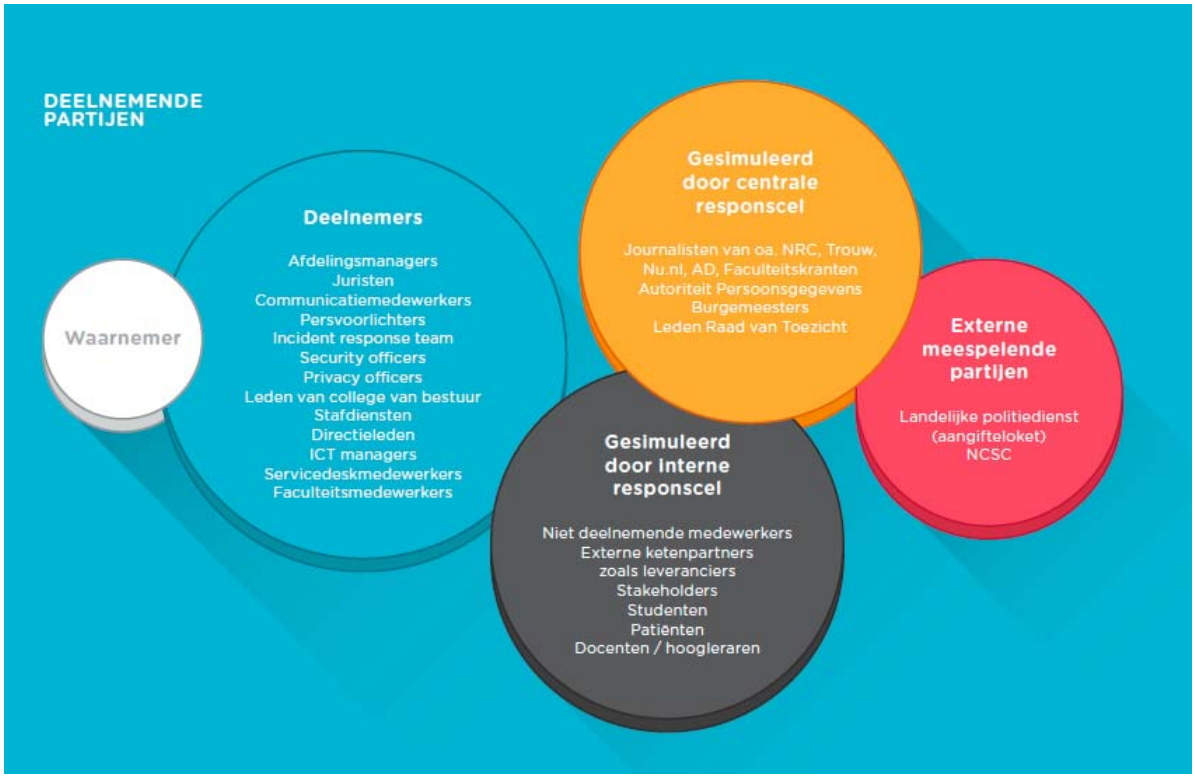
Instellingsscenario's
Het centrale scenario heeft impact op de gehele onderwijs- en onderzoekssector en creëert een instellingsoverstijgende cybercrisis. Indien meerdere instellingen meespelen kan gekozen worden om op basis van het centrale scenario instellingen een eigen instellingsspecifiek scenario te laten schrijven. Deze modulaire opzet maakt dat elke instelling de oefening aan haar eigen wensen kan aanpassen. Dit scenario is afgestemd op eigen oefendoelen: zie [bijlage 1: oefendoelen vaststellen], deelnemers en oefensituatie. Hierbij kan specifiek aandacht worden besteed aan welke informatie gevoelig ligt bij openbaarmaking en welke systemen deze informatie kan bevatten.

De ene instelling kan bijvoorbeeld geraakt worden doordat onderzoeken over dierproeven openbaar worden gemaakt, of controversiële onderzoeken naar de effecten van suiker bij kinderen; anderen kunnen bijvoorbeeld te maken krijgen bijvoorbeeld te maken het openbaren van psychologische dossiers van studenten. Bij ziekenhuizen kunnen onder meer patiëntengegevens en medicijngebruiksgegevens op straat te liggen.

Daarnaast kan declaratiegedrag van bestuurders aan de kaak worden gesteld. Dit is een enorme bedreiging voor het imago, persoonlijke reputaties, reputatie van de organisatie of kan zelfs leiden tot bestuurlijke aansprakelijkheid of financiële (schade)claims. Door dergelijke stevige technische en strategische dilemma's die niet zonder een beslissing op bestuurlijk niveau op te lossen zijn werd zowel de interne communicatie als de escalatie naar het hoogste managementniveau geoefend.

Binnen het criminele component kan bijvoorbeeld blijken dat het mogelijk is om cijfers, tentamengegevens, diplomagegevens en zelfs medicatiegegevens tegen betaling te manipuleren. Om verwarring te scheppen en de onderlinge samenwerking te stimuleren wordt niet duidelijk of hetzelfde hackerscollectief hiervoor verantwoordelijk is.

Bijlage 8: Voorbeelden rollen interne spelers en gesimuleerde rollen door responscellen



Spelers kunnen zijn:	**Gesimuleerd door Interne responscel:**	**Gesimuleerd door centrale responscel:**	**Externe meespelende partijen zoals:**
- Afdelingmanagers - Juristen - Communicatiemedewerkers - Persvoorlichters - Incident Response team - Security Officers - Privacy Officers - Leden van College van Bestuur - Stafdiensten - Directieleden - ICT managers - Servicedesk medewerkers - Faculteitsmedewerkers	- Niet deelnemende medewerkers - Externe ketenpartners - Stakeholders - Studenten - Patiënten - Docenten - Hoogleraren	- Journalisten van kranten zoals - NRC - Trouw - Nu.nl - AD - Faculteitskranten - Autoriteit Persoonsgegevens - Burgermeesters - Leden van Raad van Toezicht	- Landelijke Politiedienst - NCSC

Elke rol die niet werkelijk meespeelt kan gesimuleerd worden.

Bijlage 9: Verloop van simulatieoefening

Spelers spelen bij een simulatieoefening in de eigen omgeving een realistisch scenario na. Deelnemers oefenen zoveel mogelijk onder normale omstandigheden met eigen middelen in de eigen omgeving. Het scenario van de oefening ontwikkelt zich aan de hand van de eigen besluiten en acties.

Door de eerste interventies te verspreiden wordt het scenario in gang gezet en de eerste acties uitgezet. De responscellen doen daarna interventies om het spel op gang te houden. Deelnemers reageren hierop. Zo ontstaat een samenspel tussen de deelnemers en het scenario. De druk op de deelnemers wordt steeds groter. Dit zal leiden tot veel acties, beslissingen en communicatie.

Interventies kunnen zowel technische als strategische acties en beslissingen vereisen. Een interventie waaruit bijvoorbeeld blijkt dat er iets mis gaat bij het inloggen kan leiden tot onderzoek van de (gesimuleerde) productieomgeving. Een krantenbericht waarin gevoelige informatie openbaar is gemaakt, zal leiden tot een reactie van het college van bestuur. Met name de scenario's waarbij de deelnemers zonder strategische beslissing geen technische handeling kunnen uitvoeren, zijn interessant. In zo'n geval zullen beide niveaus actief met elkaar in gesprek moeten.

Aan het einde van de oefening zal de oefening ook weer afgeschaald en beëindigd worden. De beëindiging gebeurt door een 'freeze': een bericht naar alle spelers waarmee het spel wordt stopgezet. Tijdens de oefening kunnen zich onverwachte situaties voordoen, bijvoorbeeld wanneer iemand denkt met een echte crisis te maken te hebben of wanneer zich een echte calamiteit voordoet. Dit vergt flexibiliteit en improvisatievermogen van de oefenleider en responscellen. De oefenleider kan de oefening (tijdelijk) stilleggen.

Bijlage 10: Uitwerken technische elementen

Om een oefening zo realistisch mogelijk te maken en ook de technici voldoende te doen te geven kunnen verschillende technische componenten in de oefening geschreven en gerealiseerd worden.

Bij OZON was bijvoorbeeld een website van het hackerscollectief gebouwd bij een buitenlandse cloudprovider en werd gedurende het verloop van de oefening geactualiseerd. Op deze website verschenen datasets die bij de deelnemende instellingen zouden zijn buitgemaakt. De website werd gemirrord op verschillende plekken onder meer op Raspberry Pi's die bij een tiental instellingen verborgen waren. Sommige deelnemers hadden voor hun eigen scenario kopieën gemaakt van productieomgevingen waar de technici als "in het echt" op zoek moesten naar aanwijzingen. Logfiles van hacking activiteiten waren op de 'besmette' pc's terug te vinden. De oefenvoorbereiders hebben dit verspreid binnen hun eigen instelling. Dit logbestand vormde de basis voor de analyse van wat er gebeurd is. De logfiles werden van de command-and-control server gedownload.

Ten slotte was er voor OZON ook nog "malware" ontwikkeld die communiceerde naar een command-and-control server (Die logfiles downloadde van wat de malware zogenaamd heeft uitgevoerd.) Deze werd onder meer gebruikt voor de Capture the Flag oefening voor de brons deelnemers. Voor het verspreiden van deze malware werd gebruik gemaakt van infiltranten met een "besmette" laptop die de deelnemende "brons" instellingen bezochten.

Een belangrijke component in de oefening was het simuleren van media berichten. Met een interactieve simulator werden krantenberichten verspreid en werd Twitter en Facebook gesimuleerd waarbij de spelers ook konden reageren. Met de mediasimulator kon, net als in real-life, een veelheid aan informatie en des-informatie over de spelers uitgestort worden, waardoor de druk op de teams opgevoerd werd. Het volgen van alle media berichten was een dagtaak op zich, duidelijk een uitdaging voor de taakverdeling binnen een crisisteam.

Het technisch voorbereidingsteam bereid de technische elementen voor. Instellingen leveren informatie aan die nodig is om de technische elementen te configureren /maken en die sporen genereren. Hierbij dient rekening gehouden te worden met welke sporen er wel en niet mee worden genomen in de techniek. Voor OZON is gekozen om alle sporen vanaf 1 september mee te nemen.

Voorbeelden van technische elementen zijn:
- websites;
- malware;
- raspberry pi's om te verspreiden, deze kunnen bijvoorbeeld sites mirrorren van de websites;
- VMware;
- simulatieomgevingen van bestaande productieomgevingen;
- mediasimulator.

Bijlage 11: Spelregels spelers

Spelregels
De spelregels bevatten de regels voor het spel en de spelers.

De spelregels bevatten:
- mailadres voor communicatie tijdens spel;
- de term die gebruikt dient te worden bij elke vorm van communicatie;
- hoe mensen te benaderen die je nodig hebt tijdens het spel;
- medewerkers die meespelen zijn opgenomen in een adresboek;
- medewerkers die niet meespelen worden gesimuleerd door de interne responscel;
- de start van het spel;
- het eindigen van het spel;
- de contactpersoon bij alle vragen intern (de projectleider);
- de centrale contactpersoon bij alle vragen (oefenleider centrale spel);
- bij interrupties tijdelijk stilleggen van spel;
- bij onvoorziene omstandigheden stilleggen van spel – NO PLAY regels;
- regels voor verhindering van speldeelname;
- regels voor welk materiaal als bewijsmateriaal geldt en met name vanaf wanneer.

Verwachtingen spelers
- Het is de bedoeling dat spelers reageren zoals ze ook tijdens een gewone werkdag zouden doen.

Bijlage 12: Briefing deelnemers, organisatie en responscel

Briefing deelnemers
Licht voorafgaand aan de oefening deelnemers in over de oefening. Dit kan door middel van een bijeenkomst waarin je de spelers uitleg geeft over:
- het doel;
- de spelregels;
- de wederzijdse verwachtingen.

Dit draagt bij aan een goed verloop van de oefening.

Hiervoor kun je gebruik maken van een presentatie en uitnodiging en:
- informatiepakket;
- spelregels;
- adreslijst;
- achtergrondinformatie;
- lead in;
- teasers.

Briefing organisatie
Het kan zijn dat niet spelers binnen de organisatie geconfronteerd worden met de oefening. Je kunt ze van tevoren inlichten over dat er geoefend wordt zodat ze niet in de veronderstelling zijn dat er sprake is van een echte crisis. Wees terughoudend in het delen van details over de inhoud van de oefening, onder meer om te voorkomen dat anderen onbedoeld gaan ‘mee-oefenen.’

Briefing responscel
Voorafgaand aan de oefening kun je met de responscellen een korte start-up briefing houden. Spreek de doelen van de oefening door en stem onderling het gebruik van de ruimten, telefoons en adresboek af. Daarnaast kun je de regels voor het rollenspel bespreken en het scenario nogmaals kort doorlopen. Bespreek ook de regels voor het eventueel afbreken van de oefening.

Bijlage 13: Inhoud voor een communicatieplan

Denk na over de communicatiedoelgroepen, doelstellingen en momenten.

Doelgroepen
- **Overheid**
  Stel vragen als:
    - Is het nodig dat je richting de overheid communiceert?
    - En stel je ze alleen op de hoogte of heeft je boodschap ook nog andere inhoud?
- **Intern/Instellingen**
    - Wie wil je binnen je/de organisatie(s) bereiken met de oefening? (bestuurders, security officers, ICT-medewerkers, ICT-directeuren?)

Voor de crisisoefening
- **Interne en externe communicatie** - Deel je dat er een oefening gaat plaatsvinden en wat de inhoud is van de oefening? Bij OZON is naar de pers terughoudendheid betracht om 'mee-oefenen' te voorkomen. Intern is vlak voor de oefening aan niet-deelnemers meegedeeld dat geoefend werd waarbij de datum niet is genoemd.
- **Uitnodigen deelnemers** – nodig deelnemers op tijd uit zodat ze de tijd hebben om na te denken of ze mee willen spelen. Stel hiervoor communicatiemiddelen op met mogelijkheden, Oefendoelen en voorwaarden zoals tijd, locatie en mogelijkheden.
- **Uitnodigen interne spelers** – nodig spelers uit in hun eigen rol mee te oefenen. Stel hiervoor uitnodigingen, en briefing materiaal op om ze op de hoogte te stellen van de oefendoelen, de voordelen van mee-oefenen en vlak voor de oefening de spelregels etc.

Tijdens de oefening
- **Filmpje** - Wordt er gefilmd? (Maak hiervoor dat een apart draaiboek.) SURFnet heeft een filmpje over de crisisoefening met een overkoepelend verhaal ontwikkeld. Hierin werd vastgelegd wat de crisisoefening was, hoeveel instellingen hebben meegedaan, wat deelnemers hebben geleerd en wat de sfeer was tijdens de oefening.
- **Persberichten** - Deel je direct na de oefening dat je een crisisoefening hebt gehouden? Bij OZON is besloten om en persbericht uit te sturen waarin werd vermeld dat er een crisisoefening heeft plaatsgevonden binnen onderwijs en onderzoeksector, met het aantal instellingen dat heeft meegedaan en een aantal overkoepelende conclusies. Het persbericht is ter inzage vooraf verstuurd naar de instellingen. Het persbericht is door SURFnet verstuurd naar diverse media.
- **Artikelen** - Zijn er tijdschriften waarin je een artikel wilt plaatsen? Wie laat je deze schrijven? Eventueel een interview met een security officer, student, ICT medewerker waarin wordt aangegeven wat ze aan de oefening gehad hebben en wat ze met de resultaten gaan doen?

Na de crisisoefening
- Communiceer je intern en/of extern over **de resultaten, uitkomsten en lessons learned van de oefening**? Bij OZON is gekozen om algemene leerpunten breed te delen, maar interne leerpunten van de instellingen intern te houden.
- Zijn er **congressen en bijeenkomsten**/ andere momenten waarop je de uitkomsten wilt presenteren/delen?
- Communiceer je/en hoe communiceer je intern over de **resultaten en verbeterpunten uit de evaluaties** voor de interne crisisorganisatie?

Bijlage 14: Voorbeeld oefenprogramma cybercrisisoefening

Dag	Tijdstippen	Onderdeel oefening
Dinsdag 4 oktober 2016	8.15u – 19.00u	Decentrale deel oefening: dag 1
Woensdag 5 oktober 2016	09.00u – 12.00u	Decentrale deel oefening: dag 2
Woensdag 5 oktober 2016	14.00u – 17.00u	Centrale deel oefening: evaluatie
Woensdag 5 Oktober 2016	17.00u – 19.00u	Borrel

1.1.1.1 Oefenprogramma dag 1

Oefendag 1: Dinsdag 4 oktober			
Fase en deelnemers		**Globale tijdslijn**	**Programmaonderdelen en scenario-ontwikkelingen**
Aanloop fase	**Nadruk: technisch-operationeel niveau**	8.15 uur	Start van de oefening op de eigen locatie
			Technische Interventies scenario
			Hackers melden in media dat wat hun doel is en organisaties heeft gehackt. Het soort organisaties wordt genoemd, nog niet welke. De informatie komt later online.
			Medewerkers van organisaties geven in media aan te sympathiseren met de hackers.
			Informatie van verschillende organisaties staat online. Media duiken er op. Eerste consequenties voor de organisatie wordt duidelijk
Acute fase	**Strategische niveau betrokken (dit kan binnen een beperkt tijdspad bijv. 13.00 – 15.30 uur)**	12.30 uur	Journalist stelt telefonische vragen over (technisch deel) scenario.
		13.00 uur	In organisaties is impact van het scenario duidelijk. Dit komt mede doordat de media kritische artikelen schrijven, maar ook doordat medewerkers en klanten (studenten/patiënten/enz.) zich roeren. Interne en externe onrust.
		13.30 uur	Artikel over scenario deel komt online, organisaties worden bij naam genoemd. Het artikel is trending topic. Organisaties die niet genoemd worden, worden mogelijk wel benaderd met vragen of zij kunnen garanderen dat niet ook hun systemen zijn gehackt en gemanipuleerd (geruchten social media).
		14.00 uur	Personeel is betrokken bij verdere gegevens verspreiding (dit is afhankelijk van de keuze van de organisatie, besmetting door website bezoek of actief downloaden), mogelijk ook doordat documenten ge-maild worden naar een e-mailadres van de hackers
			Toezichthouders stellen vragen over de hackers. Enerzijds over de preparatie van de organisatie, anderzijds over situatie en maatregelen.
		14.30 uur	Speculaties vervolg acties en vervolg documenten die naar buiten kunnen komen. Hackers melden vervolg plannen op website.

		14.30 - 16.30 uur	Kritische vragen over specifieke documenten en “misstanden” binnen de organisatie worden gesteld. Online zijn zwartboeken per organisatie te vinden. Het publiek wordt gevraagd mee te bouwen aan de dossiers. Een moreel beroep wordt gedaan op het personeel om te helpen aan het opschonen van de organisaties. Enkele personeelsleden sturen niet informatie naar buiten maar rechtstreeks naar het strategische niveau om aandacht te vragen voor wat volgens hen misstanden zijn.
		17.00 uur	Einde oefendag 1

1.1.1.2 Oefenprogramma dag 2

Oefendag 2: Woensdag 5 oktober			
Fase en deelnemers		**Globale tijdslijn**	**Ontwikkeling**
Afronding en verantwoording	**Technisch-operationeel**	9.00 uur	Start van de tweede oefendag op de eigen locatie
			Vervolg scenario input. Om 12.00 uur einde oefening.
Reistijd		12.00 uur - 14.00 uur	Reistijd vanuit eigen organisatie naar centrale bijeenkomst te Utrecht
Reflectie en Evaluatie		14.00 uur	Reflectie op scenario. Gemengde teams van gelijke bloedgroepen (zoals technisch, beleid) kijken terug op het scenario aan de hand van een aantal gerichte vragen.
		15.15 uur	Pauze
		15.30 uur	Lessen trekken en verbeteren en in teams bespreken van het eigen handelen.
		17.00 uur	Plenair afsluitende reacties inventariseren
		17.30 uur	Afsluiting en borrel

Bijlage 15: Voorbeeld schema oefendagen

Oefendag 1: Dinsdag 04 oktober 2016			
Tijd	**Actie**	**Wie**	**Waar**
7.00	*Ontvangst oefenvoorbereiders voorbereiden en spelvoorbereiding* • *Check materialen* • *Laptop op schermen aansluiten* • *Telefoons aansluiten* • *Koffie/ thee klaarzetten* • *Inrichten zalen* • *Iemand van automatisering aanwezig voor ondersteuning*	*Projectsecretaris en Projectgroep*	
7.30	Ontvangst oefenvoorbereiders • Uitdelen benodigde materialen • Afstemmen rollen en taken • Opstarten Mediasimulator	Oefenvoorbereiders en Projectgroep	
8.00	Voorbereiden start oefening • Iedereen neemt positie in	Oefenvoorbereiders en Projectgroep	
08.15	START SPEL (Zie Speloverzicht/mastereventlist)		
12.00	(Eventueel) Lunch voorbereiden voor oefenvoorbereiders en projectgroep	Projectsecretaris	
12.30	Lunch (eventueel tijdens het spel)		
17.00	EINDE SPEL		
17.00	Korte interne Evaluatie		
17.30	EINDE		
	Tussentijds: Aanvullen koffie/thee		

Oefendag 2: Woensdag 05 oktober 2016			
Tijd	**Actie**	**Wie**	**Waar**
7.45	*Ontvangst oefenvoorbereiders voorbereiden en spelvoorbereiding* • *Check materialen* • *Laptop op schermen aansluiten* • *Telefoons aansluiten* • *Koffie/ thee klaarzetten* • *Inrichten zalen*	*Projectgroep*	
8.15	Ontvangst oefenvoorbereiders • Uitdelen benodigde materialen • Afstemmen rollen en taken • Opstarten mediasimulator	Oefenvoorbereiders en Projectgroep	
8.45	Voorbereiden start oefening • Iedereen neemt positie in	Oefenvoorbereiders en Projectgroep	
09.00	START SPEL (Zie Speloverzicht/ mastereventlist)		
12.00	EINDE SPEL		
12.00	Lunch (laten) voorbereiden voor oefenvoorbereiders en projectgroep		
12.30	Uitdelen lunch		
13.00	Klaarzetten ruimtes voor evaluatie		

	• *Check materialen* • *Ruimtes herindelen*		
13.30	Start ontvangst spelers @SURFnet		
14.00	START EVALUATIE		
17.00	EINDE EVALUATIE		
17.00	Borrel (laten) klaarzetten		
17.00	Borrel		
19.00	EINDE		
19.00	Start Opruimen zalen	Projectgroep	
20.00	Eventueel nazit door projectgroep (met eten?)		
	Tussentijds: Aanvullen Koffie/Thee		

Bijlage 16: Evaluatie

Evaluatie van de oefening
De uitkomsten van de oefening kunnen op verschillende niveaus geëvalueerd worden. Allereerst kan gekeken worden of het proces van de oefening goed is verlopen. De focus ligt hierbij op de organisatie van de oefening en hoe de oefening door het voorbereidende team en door de deelnemers ervaren is.

Vragen die hierbij aan de orde kunnen komen zijn:
- Hoe is de voorbereiding ervaren?
- Hoe is de intensiteit van de oefening ervaren?
- Is het scenario succesvol uitgevoerd en waren er voldoende interventies of juist te weinig?
- Heeft het scenario de gewenste impact gehad?
- Hebben de deelnemers het scenario als realistisch ervaren?
- Zijn er situaties geweest die impact hebben gehad op de uitvoering van de oefening?
- Zijn er aanbevelingen voor een volgende oefening?

Evaluatie van interne crisisprocessen
Naast de evaluatie van hoe de oefening verlopen is, kan ook geëvalueerd worden hoe en of de crisisstructuur binnen de organisatie tijdens de oefening gefunctioneerd heeft.

Hierbij kan naar het proces gekeken worden waarbij de kritische processen het uitgangspunt zijn. Beoordeeld wordt of de crisisstructuur werkt zoals beoogd. De focus ligt dan vooral op de juiste handelswijze. Ook kan gekeken worden naar de uitkomsten. De nadruk ligt op de resultaten die het oefenproces heeft opgeleverd. Hierbij gaat het vooral over de doelmatig- en doeltreffendheid van de genomen maatregelen.

Om leer- en verbeterpunten voor de crisisorganisatie vast te leggen, kan tijdens de evaluatie vragen gesteld worden als wat gebeurde er? (beschrijven), waarom gebeurde dat? (verklaren), wat zegt dat? (analyseren en reflecteren). Uit de oefening kunnen lessen getrokken worden over het verloop van de oefening en de effectiviteit van de crisisbeheersing, die de basis vormen voor het verbeteren van de interne crisisstructuur.

Een waarnemer kan de interne processen monitoren en de bevindingen inbrengen in de interne evaluatie.

Evaluatiemomenten
Plan verschillende momenten van evaluatie:
- **Tijdens het spel;** Tijdens het spel kan aan spelers een checklist/vragenlijst gegeven worden, zo kunnen ze hun bevindingen meteen monitoren. Dit kan de basis zijn voor latere evaluatiemomenten. Zo blijven belangrijke evaluatiepunten top of mind. Spelers kunnen zowel punten noteren over de oefening als punten over de interne processen.
- **Direct na het spel;** organiseer direct na het spel een evaluatiemiddag. Als je binnen één instelling speelt dan kun je zowel conclusies over het verloop van de oefening als de interne processen bespreken. Als je met meerdere organisaties speelt is het goed om te bepalen of je alleen de oefening evalueert of ook de interne processen van de organisaties. Omdat inhoudelijke processen gevoelig kunnen liggen is kan het en overweging zijn om deze slechts intern te evalueren en niet in een groep.
- **Een aantal weken na het spel;** met de oefenleiding (projectgroep, programmagroep en stuurgroep) om het verloop en de resultaten van de oefening te bespreken.

Deelnemers evaluatie
Afhankelijk van de ruimtes waar je de evaluaties houdt is het goed om van tevoren een indicatie te geven van hoeveel mensen er maximaal kunnen deelnemen aan de evaluatie. Voor OZON was het aantal gesteld op drie deelnemers per instelling. Dit zal in ieder geval de security officer zijn die ook in de programmagroep deelneemt en één of meerdere spelers.

Survey
Direct na de oefening kunnen online vragenlijsten naar de deelnemers gezonden worden met vragen over het oefenproces en/of vragen over het behalen van de (interne) oefendoelen, eigen bevindingen, succes- en leerpunten gaan.

Bijlage 17: Begrippen

Begrip	Betekenis
Master event list	Een tijdlijn waarin de interventies en acties zijn opgenomen. Deze dient als leidraad voor de oefening.
Event	Een gebeurtenis met algemene inhoud. Het aantal events hangt af van de oefendoelen. Verschillende events zijn nodig om een realistisch scenario te bereiken. [9]
Actie	De consequenties die volgen uit een event. Een actie is bedoeld om een reactie te veroorzaken bij de deelnemers. Deelnemers moeten handelen en beslissingen nemen op basis van de events. De reacties van de deelnemers brengen het scenario verder.
Interventie	Hiermee kun je acties bij de deelnemers onder de aandacht te brengen. De interventies bestaan uit sociale mediaberichten (zoals twitter), kranten en mediaberichten, telefoontjes van stakeholders, telefoontjes van journalisten en e-mailberichten van gesimuleerde contacten.
NO PLAY	Er kunnen onvoorziene situaties optreden tijdens de oefening die het niet rechtvaardigen om door te spelen. In dat geval zal de oefening gestaakt worden. De afspraken die hiervoor gelden zijn NO PLAY afspraken.
Lead In	De lead In bevat de achtergrond bij het scenario en het huidige beeld in de media en maatschappij. Deze informatie wordt voorafgaand aan de oefening doorgenomen om iedereen een gelijke start te geven.
Sitrap	“Situatie report”. Een situatie report bevat informatie op basis waarvan de situatie ingeschat kan worden, een goed beeld van de situatie gevormd kan worden en op basis waarvan beslissingen zoals opschalen genomen kan worden.
Responscel	In het scenario spelen vaak partijen of mensen een rol, die zelf niet bij de oefening betrokken zijn; denk aan journalisten, belangenverenigingen, of andere interne medewerkers. Om deze rollen wel in te zetten tijdens de oefening worden deze partijen gesimuleerd, door de ‘responscel’.

[9] ISO 22398:2013(E), art. 5.2.14, p.18

Bijlage 18: Checklist “opzetten (cyber)crisisoefening” model OZON

Simulatieoefening (goud en zilver)

Fase 1: 3 weken na start/ 37 weken voor de oefening.
- ☐ Is een projectgroep geformeerd?
- ☐ Zijn centrale doelen en oefenvorm bepaald?
- ☐ Is de datum en centrale locatie van de oefening vastgesteld en vastgelegd?
- ☐ Is er een vastgesteld budget?
- ☐ Is er een naam bedacht?
- ☐ Is er een wiki?
- ☐ Is het maximumaantal deelnemers vastgesteld?
- ☐ Vaststellen en communiceren uiterste aanmelddatum
- ☐ Zijn de deelnemers uitgenodigd?

Fase 2: 12 weken na start/ 28 weken voor de oefening.
- ☐ Hebben de deelnemers zich aangemeld?
- ☐ Is er een programmagroep geformeerd?
- ☐ Is er een stuurgroep geformeerd?
- ☐ Zijn de vergaderdata vastgelegd?
- ☐ Heb je de data van de evaluatie(s) en locatie vastgesteld en vastgelegd?
- ☐ Zijn logistiek en faciliteiten zoals de lunch tijdens de oefening geregeld?

Fase 3: 13 weken na start/ 26 weken voor de oefening
- ☐ Hebben de deelnemers de oefendoelen en scope van de oefening bepaald?
- ☐ Is er een need/nice to have list gemaakt voor het scenario van de oefening?

Fase 4: 16 weken na de start/ 24 weken voor de oefening
- ☐ Is er een keuze gemaakt voor het gesloten systeem voor distributie van mediaberichten (e-mail of mediasimulator?)
- ☐ Is het centrale scenario vastgesteld?
- ☐ Is vastgesteld welke technische elementen nodig zijn, en is duidelijk wat gekocht en/of gebouwd moet worden?
- ☐ Heb je een communicatiestrategie en communicatieplan?
- ☐ Is er een gezamenlijke persstrategie?
- ☐ Stel vast of je gebruik wilt maken van waarnemers

Fase 5: 27 weken na de start/ 13 weken tot aan de oefening
- ☐ Heb je een globale dagplanning van de oefendagen?
- ☐ Is het instellingsscenario globaal vastgesteld?

Fase 6: 35 weken na de start/ 5 weken voor de oefening
- ☐ Als externe partijen meespelen, zijn ze uitgenodigd?
- ☐ Is het centrale scenario uitgewerkt in de master event list?
- ☐ Hebben de instellingen de scenario’s uitgewerkt in een master event list?
- ☐ Zijn alle centrale spelelementen/interventies uitgewerkt?
- ☐ Zijn alle instellingsspecifieke elementen/interventies uitgewerkt?
- ☐ Zijn de technische elementen/interventies uitgewerkt?

- ☐ Is de documentatie uitgewerkt? Denk aan;
  - ☐ Lead in
  - ☐ Informatiepakket spelers

- ☐ E-mail richting organisatie
- ☐ Materiaal voor briefing spelers
- ☐ E-mail uitnodiging spelers
- ☐ Adreslijst
- ☐ Eventueel Teasers

- ☐ Zijn de communicatiemiddelen (e-mailadressen/jabber etc.) geactiveerd en werkzaam?
- ☐ Zijn de waarnemers aangesteld?

- ☐ Zijn de technische hulpmiddelen getest/verspreid en functionerend?
  - ☐ Raspberry Pi
  - ☐ Logfiles
  - ☐ Malware
  - ☐ Websites
  - ☐ Simulatieomgeving van de productieomgeving

Fase 7: 38 weken na de start/ 2 weken voor de oefening
- ☐ Zijn de interne spelers uitgenodigd?
- ☐ Hebben de spelers een briefing gehad?
- ☐ Hebben de responscellen een briefing gehad?
- ☐ Is de documentatie onder de spelers verspreid?
- ☐ Is de organisatie op de hoogte gesteld van dat er een oefening zal plaatsvinden?
- ☐ Zijn de persberichten voorbereidt en voorlichters geïnstrueerd?

Fase 8: 39 weken na de start/ 1 week tot de oefening
- ☐ Zijn alle interventies ingevoerd in de gesloten mediaomgeving, staan alle interventies klaar voor de oefening?

Fase 9: 40 weken na de start/ 0 weken tot de oefening
- ☐ Uitvoering Oefening
- ☐ Hot wash evaluatie

Fase 10: in een periode van 0 tot 4 weken na de oefening.
- ☐ Evalueren en uitwerken van evaluatie
- ☐ Uitkomsten communiceren binnen de instelling(en)

Voor de Capture the Flag (bronsoefening)
Extra aandachtspunten wanneer gelijktijdig met de simulatieoefening een Capture the Flag wordt uitgevoerd.

Fase 3: 13 weken na de start/ 27 weken voor de oefening
- ☐ Bronsoefening - Is een oefenvoorbereider bij de bronsinstellingen aangesteld?

Fase 6: 35 weken na de start/ 5 weken voor de oefening
- ☐ Zijn de infiltranten geregeld?
- ☐ Is de aanvalssoftware voor de ‘Capture the Flag’ oefening klaar?

Fase 7: 38 weken na de start/ 2 weken voor de oefening
- ☐ Zijn de infiltranten in het bezit van de infiltratiesoftware?
- ☐ Zijn de infiltranten gebrieft over de taken?
- ☐ Zijn de bronsinstellingen gebrieft over gebruik mediasimulator/ontvangst e-mails en over de Capture the Flag oefening?
- ☐ Hebben de infiltranten een vrijwaringsbewijs ontvangen?