Samen aanjagen van vernieuwing

Handleiding NOZON2019

Samen crisis creëren

Auteur(s):	Charlie van Genuchten
Versie:	1
Datum:	2 mei 2019

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
info@surf.nl
www.surf.nl

Inhoudsopgave

1 Inleiding

Dit document is in eerste instantie geschreven als informatiepakket bij de NOZON oefenweken in 2017 en is uitgebreid voor NOZON 2019 met nieuwe voorbeeld-scenario's. De opzet van NOZON is simpel: elke instelling organiseert in dezelfde twee weken zelf een korte table-top oefening met behulp van centraal aangeleverd materiaal. Elke instelling wijst voor het organiseren en evalueren van de oefening een oefenvoorbereider en waarnemer aan, die voorafgaand aan de oefening een training krijgen en worden gefaciliteerd in sparren met andere instellingen.

Dit document is bedoeld als handleiding om een goede oefening te kunnen organiseren met de voorbeeldscenario's die voor NOZON ontwikkeld zijn. Hierbij gaan we eerst terug naar de basis en nemen we daarna de voorbereiding, uitvoering en evaluatie van een oefening door.

Begrippenlijst
Onderstaand een korte begrippenlijst om verwarring te voorkomen.

De oefenvoorbereider is degene die de oefening voorbereidt en leidt. De oefenvoorbereider kan dus zelf niet meespelen, aangezien hij/zij het scenario kent. Dit zijn mensen die deze rol goed zouden kunnen invullen:

- Integrale veiligheidsmanager;
- Business Continuity Manager;
- Crisiscoördinator;
- Degene die de overige crisisoefeningen ook organiseert;
- Incidentmanager;
- Security officer.

De waarnemer stelt voorafgaand aan de oefening samen met de oefenvoorbereider een evaluatieplan op en zal tijdens de oefening waarnemen of de verwachte acties worden genomen en de afgesproken procedures worden gevolgd. De waarnemer zal niet kunnen deelnemen aan de oefening en zal ook niet helpen in de spelleiding. Het is voor deze rol daarom vooral van belang dat deze persoon de eigen crisis- en incidentprocedures goed kent en in staat is goed te beschrijven welke stappen de oefening doorloopt.

Het oefenteam is de benaming voor de groep mensen die deelnemen aan de oefening. Zij mogen van tevoren niets weten over de inhoud van de oefening. Wel zullen vooraf onder andere de spelregels voor tijdens de oefening gedeeld worden.

De responscel is de benaming voor de persoon (of groep personen) die de oefenvoorbereider helpt met het realistisch gaande houden van de oefening. Deze mensen geven tijdens de oefening nieuwe informatie en stellen vragen aan het oefenteam. Zij mogen van tevoren de gehele oefening en het hiervoor opgestelde draaiboek kennen en worden geacht hun rol voor te bereiden.

Injects zijn de acties van de responscel om de oefening gaande te houden of een nieuwe wending te geven. Als een gesimuleerde journalist bijvoorbeeld belt met vragen over de crisis is dat een inject.

Overzicht bijlages

Dit document is opgebouwd uit een handleiding met 8 bijlages. De **eerste vier bijlages** zijn checklists en templates die kunnen worden gebruikt in de voorbereiding en evaluatie van de oefening.

Bijlages 5 t/m 8 zijn voorbeeldscenario's op IT en Strategisch niveau, waarbij je kunt kiezen uit:

- Casus: hack bij een cloudleverancier (Bijlage 5 en 7), of
- Casus: identiteitsfraude en data integriteit (Bijlage 6 en 8)

2 De basis

2.1 Table-top oefening

In het whitepaper van OZON staat een uiteenzetting van alle soorten oefeningen die men kan organiseren. Table-top oefeningen staan daarin als volgt beschreven:

Bij een table-top 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 table-top relevante informatie delen, overzicht krijgen en (adequate) besluiten en (communicatie)maatregelen nemen. Een table-top is een goede optie als men in relatieve rust de crisisstructuur en de onderlinge samenwerking wil oefenen en/of specifieke vaardigheden wil trainen.

Meestal wordt bij een table-top oefening de groep mensen die gaan oefenen in één ruimte gezet. Zij krijgen aan het begin van de oefening informatie over de crisis die op dat moment gaande zou zijn en moeten beslissingen maken op basis van de informatie die ze tijdens de oefening gegeven wordt. Een table-top is van korte duur, waardoor de crisis in een korte tijd moet worden opgebouwd en afgehandeld.

2.2 Stappen in het organiseren van een oefening

Het organiseren van de oefening kan worden opgedeeld in de stappen: voorbereiding, uitvoering en evaluatie. Hieronder is uitgezet wat er onder die verschillende stappen valt. Deze lijst is ook als aanpasbare checklist terug te vinden als **Bijlage 1** bij dit document.

Voorbereiding

- Aanwijzen oefenvoorbereider en waarnemer;
- Vaststellen doelstellingen oefening;
- Datum en tijd bepalen voor de oefening;
- Uitwerken scenario voor eigen organisatie;
- Bepalen en betrekken oefenteam;
- Bepalen en betrekken responscel;
- Ruimtes reserveren voor het oefenteam en de responscel;
- Uitwerken evaluatievragen;
- Korte doorloop oefening met de responscel.

Uitvoering

- Een paar dagen van tevoren een reminder naar het oefenteam;
- Een paar dagen van tevoren een reminder naar de responscel;

- Begin oefening: casus en aanpak oefening toelichten aan het oefenteam;
- Responscel instrueren voor injects;
- Waarnemen oefening.

Evaluatie

- Hot wash, gelijk na de oefening: eerste reacties oefenteam en responscel ophalen (mondeling);
- Uitwerken eigen observaties en observaties oefenteam en responscel in adviesdocument;
- Vastleggen en presenteren advies aan de relevante groep(en);
- Lessons learned formuleren;
- Verbeteringen benoemen en vervolgacties uitzetten.

3 Voorbereiding

3.1 Vaststellen doelen

Stel voor jouw instelling vast wat je uit deze oefening wil halen. Stem dit eventueel af met relevante managementlagen. Je oefening kan als doel hebben om:

- Bewustwording te creëren;
- Kennis en vaardigheden te verbeteren;
- Samenwerking te verbeteren;
- Te experimenteren met nieuwe processen of werkwijze;
- En/of een proces te testen.

Kies één of een aantal van bovenstaande doelen en verscherp voor jouw instelling wat dit betekent (om welk proces gaat het, wiens kennis, vaardigheden of samenwerking moet worden verbeterd etc.). Bepaal daarna hoe je deze doelen gaat behalen met de oefening.

Tips

- Zorg dat je niet te veel doelen hebt voor één oefening. Bij meer dan vijf doelen wordt het moeilijk om gericht te observeren en evalueren.
- Gebruik de leerpunten van de vorige oefening die je hebt gehad als doelen voor deze oefening.
- Als het de eerste oefening met dit team is, gebruik de oefening dan vooral als een eerste test hoe de samenwerking gaat.

Keuze: nadruk op het oefenen van procedures of het oefenen van reactiesnelheid
De scenario's zijn nu in een draaiboek gegoten van ongeveer één uur waarbij er wordt uitgegaan van een ingeplande oefening met een aangekondigd begin en einde. Dit heeft de toegevoegde waarde dat je in een korte tijd kan kijken of vastgestelde procedures worden gevolgd en dat iedereen die officieel bij zo'n incident betrokken zouden moeten zijn mee kan oefenen.

Mocht één van de oefendoelen echter zijn om te kijken hoe snel men reageert op indicaties van een crisis, kan ervoor worden gekozen om niet precies aan te geven wanneer de oefening plaats gaat vinden en kan het scenario worden aangepast met een langere aanloop. Let hierbij wel op dat het moeilijker zal zijn voor de waarnemer om te zien wat er allemaal voor acties worden ondernomen.

3.2 Uitwerken scenario

Als je de oefendoelen van jouw instelling hebt vastgesteld, kun je het scenario verder gaan aanpassen en uitwerken. De voorbeeldscenario's vind je in **Bijlage 5 t/m 8**. De scenario's beginnen met een inleiding van de casus: wat is de crisis. Daarna komt volgt het draaiboek waarin je per 5/10 minuten injects kan verwerken.

Vragen om jezelf te stellen om de casus uit te werken:

- Welk systeem wordt geraakt?
- Wat voor impact heeft dit op jouw instelling?
- Welke processen moeten worden stopgezet?
- Welke data worden aangepast?

Vragen om jezelf te stellen om het draaiboek uit te werken:

- Welke stakeholders worden geraakt door de casus?
- Hoe zouden interne betrokkenen hierop reageren?
- Hoe zouden externe betrokkenen hierop reageren?
- Zou de media betrokken raken en zo ja, hoe?
- Welke informatie heeft het oefenteam nodig om beslissingen te maken?
- Welke stappen moet het oefenteam doorlopen om je doelstellingen te behalen?

Tips

- Probeer in ieder geval een aantal mensen (die niet in het oefenteam zitten) een keer mee te laten kijken naar je scenario, zodat je van meerdere invalshoeken een check hebt of het verloop van het scenario realistisch is.
- Plan niet je hele draaiboek per minuut vol, want uiteindelijk zullen er altijd onverwachte dingen gebeuren tijdens de oefening, waardoor alles sneller of langzamer gaat dan verwacht en je samen met de responscel zal moeten improviseren.
- Bij het strategische scenario, denk goed na over de zaken die op strategisch niveau gevoeld zullen worden: claims, persoonlijke reputatie, reputatie organisatie, bestuurlijke aansprakelijkheid en ethische kwesties.
- Leg de crisis- en incidentprocedures naast de verwachte acties in het scenario. Als er bijvoorbeeld pas naar het strategische niveau moet worden geëscaleerd als er sprake is van de dreiging van meer dan 4 uur uitval van een kritisch bedrijfsproces kun je dit erbij zetten om te zien of er niet te

snel of te laat wordt geëscaleerd.

Optie: Tijdsprong
Degenen die al een aantal oefeningen hebben georganiseerd en een extra uitdaging willen geven aan het oefenteam, kunnen overwegen om een tijdsprong in het scenario toe te voegen. In de scenario's in **Bijlage 6 en 8** is een voorbeeld van een tijdsprong opgenomen. Deze aanpassing kan ervoor zorgen dat het oefenteam beter moet nadenken over het zomaar uitzetten/offline halen van een systeem.

3.3 Oefenteam en responscel betrekken

Bij de vier scenario's in de bijlages staan overzichten van de rollen die in het oefenteam en responscel aanwezig kunnen/moeten zijn. Pas deze aan naar de rollen in het door jouw aangepaste scenario. Bepaal de precieze samenstelling van je oefenteam en responscel zo ver mogelijk voor de oefening en leg het oefenmoment in ieder geval bij je responscel vast in de agenda. Als je niet voor een verrassingseffect gaat is het belangrijk de oefening ook tijdig vast te leggen in de agenda van je oefenteam.

3.4 Uitwerken evaluatievragen

Om tijdens de oefening de observaties van de waarnemer gelijk te kunnen koppelen aan de oefendoelen is het van belang om voorafgaand aan de oefening uit te werken welke vragen de waarnemer zichzelf kan stellen. Gebruik hiervoor het formulier waarneming in **Bijlage 2**.

4 Uitvoering en evaluatie

4.1 Setting

Een klassieke table-top oefening wordt gehouden met het oefenteam in één ruimte aan een vergadertafel en de responscel in een ruimte daarnaast. De oefenvoorbereider en waarnemer zitten in de ruimte bij het oefenteam en de oefenvoorbereider geeft extra aanwijzingen digitaal door aan de responscel. De **strategische scenario's** (**Bijlage 7 en 8)** gaan van deze setting uit.

De **IT-scenario's (Bijlage 5 en 6)** gaan ook van deze setting uit, met het verschil dat het oefenteam in een ruimte zit die groot genoeg is om op te kunnen splitsen in verschillende groepen. Daarbij is er dus minder sprake van een vergadersetting. De responscel zit daarbij nog steeds in een ruimte ernaast.

4.2 Doornemen oefening met responscel

Neem voorafgaand aan de oefening met de mensen uit je responscel het scenario door en besteedt daarbij in ieder geval aandacht aan het volgende:

- Neem met de responscel door of de geplande acties realistisch en logisch zijn gezien het desbetreffende incident.
- Zorg ervoor dat je per rol hebt uitgewerkt wie wat wanneer zegt.
- Neem met de responscel door op welke manier zij hun injects uitvoeren. Moet elk persoon bijvoorbeeld naar binnenlopen? Of laat je hen allemaal bellen? Probeer voor de overzichtelijkheid van deze oefening te beperken dat injects via de mail verlopen.
- Druk je responscel op het hart om niet zelf te gaan improviseren: de oefenvoorbereider beslist tijdens de oefening of er een extra inject nodig is en geeft dit door aan de responscel.

4.3 Spelregels tijdens de oefening

Neem met je oefenteam en responscel voorafgaand aan de oefening de volgende spelregels door:

- Start iedere communicatie zoals telefoongesprek, email of gesprek met "Crisisoefening".
- Als je contact wil opnemen met iemand die niet in de responscel zit, kan de oefenvoorbereider ervoor kiezen om deze persoon te (laten) simuleren
- De start en het einde van de oefening worden aangegeven door de oefenvoorbereider.
- Als er zich een echte crisis voordoet tijdens de crisisoefening, geeft de oefenvoorbereider dit aan met de woorden NO PLAY.
- Mocht je tijdens de oefening zelf verhinderd zijn, neem dan contact op met je oefenvoorbereider. In samenspraak draag jij zorg voor vervanging.

Deze spelregels kun je ook van tevoren rondsturen naar de betrokkenen in de vorm van een briefing. In **Bijlage 4** kun je een voorbeeld van zo'n briefing vinden.

4.4 Rollen oefenleider en waarnemer tijdens de oefening

Tijdens de oefening zal de oefenleider bij het oefenteam aanwezig zijn en contact houden via chat of mail met de responscel. Hij/zij kan er ook voor kiezen om tussen het oefenteam en de responscel heen en weer te lopen. Tijdens de oefening zal de oefenleider het scenario in de gaten houden en zorgen dat de crisis door meer of minder injects sneller of langzamer verloopt.

Tijdens de oefening zal de waarnemer constant bij het oefenteam in de ruimte aanwezig zijn. Hij/zij houdt op het formulier waarneming (**Bijlage 2**) bij wat er tijdens de oefening gebeurt.

Taken van de waarnemer:

- luisteren, aandacht voor verbale en non-verbale signalen
- ziet het effect van gedrag van één deelnemer op andere deelnemers
- maakt onderscheid tussen feitelijk gedrag en aannames
- legt verbanden op basis van de gegeven teamdynamiek
- signaleert (potentiële) problemen / knelpunten inzake het teamproces
- destilleert individuele / team competenties uit gedrag
- houdt overzicht en verdeelt zijn aandacht over de verschillende deelnemers

Het is daarbij van belang om in de verslaglegging een duidelijk verschil te maken tussen waarneming en oordeelsvorming. Sommige instellingen bij NOZON2017 werkten met twee waarnemers om een betere en objectievere verslaglegging te garanderen.

4.5 Uitwerken en presenteren evaluatie

De waarnemer werkt na de oefening zijn/haar observaties en die van alle aanwezigen samen met de oefenvoorbereider uit in een adviesdocument. Gebruik hiervoor het template in **Bijlage 3**. Zorg ervoor dat de geformuleerde adviezen zo snel mogelijk worden gedeeld binnen de organisatie. Plan hiervoor als het mogelijk is gelijk een moment in om met de relevante mensen het adviesplan door te lopen. Zorg er daarnaast voor dat je een verslag van de oefening op intranet plaatst, om zoveel mogelijk awareness in je organisatie te bewerkstelligen.

Bijlage 1 Checklist organisatie oefening

Actie	**Verantwoordelijkheid**	**Deadline**
Aanwijzen oefenvoorbereider en waarnemer	Instelling	
Vaststellen doelstellingen	Oefenvoorbereider en waarnemer	
Datum en tijd bepalen	Oefenvoorbereider	
Aanpassen scenario	Oefenvoorbereider	
Bepalen en betrekken oefenteam	Oefenvoorbereider	
Bepalen en betrekken responscel	Oefenvoorbereider	
Ruimtes reserveren	Oefenvoorbereider	
Uitwerken evaluatievragen	Waarnemer	
Korte doorloop oefening met responscel	Oefenvoorbereider	
Reminder oefening naar oefenteam	Oefenvoorbereider	
Reminder oefening naar responscel	Oefenvoorbereider	
Houden van de oefening	Oefenvoorbereider/ Waarnemer	
Uitwerken evaluatie	Waarnemer / Oefenvoorbereider	
Presenteren evaluatie	Waarnemer / Oefenvoorbereider	

Bijlage 2 Formulier waarneming

In dit document wordt de taak van de waarnemer van de table top oefening omschreven. Hiervoor zijn oefendoelen opgesteld waarop gelet moet gaan worden.

Leerdoelen voor deze table top oefening zijn de volgende: [VUL DE GEKOZEN LEERDOELEN IN, ONDERSTAAND VOORBEELDEN]

- Is het proces vanaf het constateren van een beveiligingsincident (crisis) goed ingericht.
- Zijn de juiste mensen (stakeholders) betrokken; weten ze dat ze een rol hebben, welke rol en is die duidelijk genoeg
- …

Om deze te beantwoorden zijn de volgende subdoelen vastgesteld: [STEL SUBDOELEN OP, ONDERSTAAND VOORBEELDEN]

- Is duidelijk wie waarvoor verantwoordelijk is
- Hoe gaat de impactanalyse van het crisisteam?
- Wordt er aan damage control gedaan (indien nodig)?
- Worden de juiste stakeholders op tijd ingeschakeld?
- Hoe wordt bepaald of er geescaleerd moet worden en wie bepaalt dat?
- Hoe verloopt escalatie?
- Hoe verloopt het proces na escalatie (hoe wordt met verantwoordelijkheden omgegaan en hoe vindt besluitvorming plaats)?

De oefening wordt geleid door de oefenleider en zal een waarnemer hebben.

Taken van de waarnemer:

- luisteren, aandacht voor verbale en non-verbale signalen
- ziet het effect van gedrag van één deelnemer op andere deelnemers
- maakt onderscheid tussen feitelijk gedrag en aannames
- legt verbanden op basis van de gegeven teamdynamiek
- signaleert (potentiële) problemen / knelpunten inzake het teamproces
- destilleert individuele / team competenties uit gedrag
- houdt overzicht en verdeelt zijn aandacht over de verschillende deelnemers

Hierbij kan hij/zij gebruik maken van onderstaande tabellen: [PAS EVENTUEEL TABEL AAN OP OEFENDOELEN]

Oefendoelen	**Criteria inhoud oefendoelen**	**Observatie**	**Analyse**	**Beoordeling (zie dropdown)**	**Aanbevelingen**
Algemeen					
Stakeholders	Zijn de juiste stakeholders aanwezig en kennen ze hun rol? Duidelijk wie waar verantwoordelijk voor is?				
Structuren crisis / coordinatie	Is alle info van het incident bekend? Is er bekend waar men de info kan halen?				
Proces					
Beeldvorming van de crisis	Hoe gaat de impact analyse?				
Coordinatie van het incident	Aansturing is overzichtelijk? Duidelijkheid in de coordinatie (Wie stuurt wie aan)				
Onderscheid van oorzaak en gevolg	Oorzaak en gevolg worden duidelijk neergezet?				
Onderscheiden Strategisch en operationeel niveau	Er wordt duidelijk onderscheid gemaakt tussen Strategisch en operationeel niveau. Zaken die bij Operationeel / technisch thuishoren worden correct en snel doorgespeeld?				

Procedures					
Overleg tussen verschillende afdelingen en leveranciers	Er wordt snel en efficient met de beheerorganisatie en leveranciers gecommuniceerd				
Informatie management	Wie bepaalt wat en wanneer er gecommuniceerd moet worden? Zijn de juiste communicatiemensen aanwezig?				

Gedrag	**Voorzitter**	**Deelnemer1**	**Deelnemer2**	**Deelnemer3**	**Groepsgedrag**
Interactie met anderen (luisteren en spreken)					
Houding - Actief - Passief - Rustig - Onrustig					
Besluitvorming					
Overig					

Logboek

Het kan zijn dat de acties van het oefenteam tijdens de oefening door een secretaris worden bijgehouden. Mocht dit niet het geval, is het aan de waarnemer om dit tijdens de oefening te doen. In dat laatste geval kan hij/zij het scenario nemen en een extra kolom toevoegen om de reacties en acties per inject bij te houden.

Evaluatiepunten oefenteam

Hier schrijft de waarnemer na de oefening de algemene observaties van het oefenteam op.

Wat was er opvallend?

Wat ging goed?

Wat kan beter?

Evaluatiepunten responscel

Wat was opvallend?

Wat ging goed?

Wat kan beter?

Vervolgacties

Hier schrijft de waarnemer de vervolgacties op die uit de directe evaluatie komen.

Bijlage 3 Template adviesdocument

Inleiding en doelstelling
Op [DATUM] heeft een cyber-crisisoefening plaatsgevonden. Deze oefening had tot doel:

- [OEFENDOEL 1]
- [OEFENDOEL 2]
- [OEFENDOEL 3]
- …

Aan de crisisoefening hebben de volgende personen deelgenomen:

- [AANWEZIGE 1]
- [AANWEZIGE 2]
- [AANWEZIGE 3]
- …

De oefening is geobserveerd door [NAAM EN FUNCTIE WAARNEMER]

De oefening was voorbereid door [NAAM EN FUNCTIE OEFENVOORBEREIDER]

In dit verslag worden de uitkomsten van deze oefening vastgelegd.

Casus

De oefening is gehouden op [DATUM EN TIJDSTIP]. De oefening betrof de volgende casus:

[KOPIEER HIER DE UITEINDELIJKE CASUS VAN DE OEFENING]

Zie logboek verloop van de oefening paragraaf 6.

Observaties per oefendoel
[OEFENDOEL 1]

- [OBSERVATIE 1]
- …

[OEFENDOEL 2]

- [OBSERVATIE 1]

Bevindingen oefenteam
- [OBSERVATIE 1]
- [OBSERVATIE 2]
- …

Bevindingen responscel
- [BEVINDING 1]
- [BEVINDING 2]
- …

Conclusie en aanbevelingen
Conclusie

- [CONCLUSIE 1]
- [CONCLUSIE 2]

Aanbevelingen

- [AANBEVELING 1]
- [AANBEVELING 2]
- …

Logboek verloop oefening

[KOPIEER HIER HET LOGBOEK VAN DE OEFENING]

Bijlage 4 Briefing

Beste Collega's

Hoewel we in onze ICT omgeving gelukkig niet heel vaak te maken hebben met grote incidenten is het toch belangrijk om voorbereid te zijn als zo'n incident zich wel een keer zou voordoen. Daarom gaan we [DATUM of TIJDSBESTEK invullen] een cyber-crisisoefening houden.

Lees deze mail goed door want er staan een aantal spelregels in die voor een ieder van jullie van belang zijn.

Ook al is er geprobeerd het scenario zo realistisch mogelijk te houden, het kan altijd voorkomen dat er gebeurtenissen plaats vinden die wellicht minder realistisch zijn. Ten behoeve van de oefendoelen gaan we daar tijdens de oefening geen discussie over voeren maar nemen we de gebeurtenis als "waar" aan.

Omdat we het hele proces van melding tot oplossing willen oefenen is gekozen voor een verrassingsoefening. Vanaf het moment dat de Servicedesk anderen gaat inschakelen gaan we over naar een table-top oefening. Tijdens een table-top oefening zit het oefenteam in één ruimte waarbij er beslissingen genomen worden op basis van informatie die tijdens de oefening wordt gegeven. [PAS DIT GEDEELTE AAN NAAR EIGEN INSTEEK VAN DE OEFENING]

Het oefenteam is niet vooraf bepaald maar kan dynamisch gevormd worden vanuit de afdelingen ICT en IM. [PAS DIT GEDEELTE AAN NAAR EIGEN INSTEEK VAN DE OEFENING]

Naast het oefenteam is er ook een responscel ingericht. De responscel helpt bij het realistisch gaande houden van de oefening. De personen in de responscel geven tijdens de oefening nieuwe informatie maar kunnen ook vragen stellen.

In de ruimte van het oefenteam is de oefenleider [NAAM OEFENLEIDER] en een waarnemer [NAAM WAARNEMER] aanwezig.

Om de oefening goed te laten verlopen spreken we de volgende spelregels met elkaar af.

- Start iedere communicatie zoals telefoongesprek, email of gesprek met "Crisisoefening".
- De eerste persoon die door de Servicedesk wordt ingeschakeld met het bericht "crisisoefening" loopt direct naar de oefenleider (Anita). Vervolgens wordt samen de oefenruimte opgezocht en zal de tabletop oefening van start gaan. [PAS DIT GEDEELTE AAN NAAR EIGEN INSTEEK VAN DE OEFENING]
- Als je gevraagd wordt je bij het oefenteam te voegen dan doe je dat en laat je het werk waar je op dat moment mee bezig bent rusten. (ook als je in vergadering zit)
- Als het oefenteam contact wil opnemen met iemand die niet in de responscel zit, kan de oefenleider ervoor kiezen om deze persoon te (laten) simuleren
- De start en het einde van de oefening wordt aangegeven door de oefenleider.

Als er zich een echte crisis voordoet tijdens de crisisoefening, dan wordt dat aangegeven met de woorden NO PLAY.

Bijlage 5 IT Scenario Cloudleverancier

Casus oefening – IT

Vandaag, [datum], is om [tijdstip] bij de [helpdesk] van [instelling] een melding van een administratiemedewerker van de [afdeling] binnengekomen. Medewerkers van de [afdeling] kunnen niet in het systeem [cloud systeem] van de leverancier [leverancier]. De foutmelding die de medewerkers te zien krijgen is zoiets als: “systeem is onbereikbaar”. Zonder toegang tot dit systeem kan de [afdeling] hun werk niet uitvoeren, waardoor het [prmaire bedrijfsproces] volledig stil komt te liggen.

Het getroffen systeem is een cloudoplossing dat in 2014 [of eerder] via [Surfconext/SSO/I&AM] is aangesloten en in gebruik is genomen bij de [instelling]. De gebruikers kunnen met eigen instellings-ID credentials in het systeem inloggen. In het systeem wordt door de medewerkers van de [afdeling] belangrijke data opgeslagen en verwerkt. De data uit dit systeem wordt middels verschillende koppelingen [bijv. service bus] verder ontsloten naar andere systemen en databases; zoals bijvoorbeeld naar BI t.b.v. corporate rapportages maar ook naar operationele systemen [Osiris/SAP/Blackboard/CRM/CMS/EPD/….] voor verwerking van […inschrijvingen/personeelsdossiers/klantengegevens/patientendossiers….].

Er is door de [helpdesk] nog geen contact geweest met de cloud leverancier. [helpdesk] heeft de melding wel doorgezet naar de betreffende interne functionele applicatiebeheer-team. Systeem staat op de lijst van de meest bedrijfskritieke systemen binnen de [instelling]. De applicatiebeheerder heeft de melding zojuist geëscaleerd naar de Prio 1 incident team.

Draaiboek IT scenario

Plaats van de oefening

Bij voorkeur in één ruimte. Ruimte moet voldoende groot zijn om het oefenteam in 2 groepen te kunnen splitsten en separaat aan een deel-opdracht te laten werken. Een break-out ruimte in de buurt kan ook handig zijn.

Start van de oefening

Oefening start op een vooraf aangekondigde moment en plaats. Het oefenteam wordt in deze ruimte bij elkaar geroepen middels een uitnodiging in de agenda. Hier wordt het scenario uitgelegd, waarna de oefening start.

Optioneel: oefening laten starten op een niet aangekondigde moment, waardoor er een extra verassingselement onderdeel wordt van de oefening. Daarmee kan de snelheid van de reactie, maar ook aanwezigheid van key-personen en/of hun vervangers worden getest.

Rollen in het oefenteam	**Rollen in de responscel**
• 1e lijn IT support medewerker • 2e lijn IT support medewerker • Applicatiebeheerder • Koppelingenbeheerder • Hoofd/coördinator applicatiebeheer • Incident manager / Prio 1 coördinator • Voorzitter CERT • Security officer / specialist • CERT leden • Contract beheerder • Service (level) manager • Communicatiemedewerker • Manager/directeur ICT • …	• Medewerker administratie • Accountmanager cloud leverancier • Functioneel beheerder • Student • Onderzoeker • Bestuurssecretaris • Strategisch Calamiteitenteam • Coördinator integrale veiligheid • Jurist / privacy officer • CISO • Spelleider • Waarnemer *Als het oefenteam contact wil opnemen met iemand die niet in de responscel zit moet de spelleider deze persoon simuleren of aangeven dat deze persoon niet bereikbaar is.*

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
Start ongeplande oefening (oefening waarbij startmoment niet vaststaat, maar start een verassingselement is)				
Dag vooraf of via mail	Briefing in geval van oefening waar startmoment niet vast staat: de context, spelregels, tools, etc. van de oefening uitleggen.		Oefenleider	
13:50	Start ongeplande oefening (oefening waar startmoment niet vaststaat, maar start een verassingselement is). Medewerker administratie belt met de [helpdesk], geeft codewoord Crisisoefening en vertelt dat haar/zijn systeem niet bereikbaar is.	Helpdesk medewerker neemt de melding aan, registreert het in het systeem. Helpdesk medewerker vraagt door, analyseert de melding en constateert dat het om een systeem gaat dat een kritisch bedrijfsproces ondersteund.	Medewerker administratie	Hoi Helpdesk, ik kom niet in mijn systeem. Ook al mijn collega's kunnen het systeem niet in. We krijgen de melding: systeem is onbereikbaar. Wanneer gevraagd, verteld de medewerker dat systeem een kritisch bedrijfsproces ondersteunt.
13:55	[helpdesk] escaleert de melding naar de 2e lijn. Security aspecten nog niet in beeld.	Escaleren van de melding naar 2e lijn. Bij voorkeur ook prioriteiten als een PRIO 1 melding, dus activeren van emergency/prio 1 procedures. Duur: max 5 minuten.	1e lijn IT support	

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:00	Applicatiebeheerder geeft de melding een prio 1.	Inschakelen ICT PRIO 1 team. Inschatting geven van impact en time- to-repair.	Applicatiebeheerder	

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
Start geplande oefening (oefening waarbij alle deelnemers al in één ruimte zitten)				
13:50	Briefing bij de oefening waarbij alle deelnemers al in één ruimte zitten: de context, spelregels, tools, etc. van de oefening uitleggen.		Oefenleider	
14:00	De oefenleider roept het oefenteam bijeen in het crisiscentrum. De oefenleider vertelt over de calamiteit en de reden van de bijeenkomst.	De oefenleider geeft briefing over de situatie.	Oefenleider	De oefenleider leest de casus voor en licht deze toe. Cloud leverancier [leverancier] levert een dienst aan de organisatie. De dienst is niet meer bereikbaar. Dit raakt een kritisch bedrijfsproces.

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:05	De contactpersoon van de organisatie belt de cloudleverancier om te achterhalen wat er aan de hand is.	Achterhalen: Wat precies het probleem is Wat hieraan kan worden gedaan Hoe lang dit duurt Wat de impact is	Accountmanager Cloud leverancier	De medewerker geeft aan dat hij niet zeker weet of hij het wel mag vertellen maar dat ze waarschijnlijk gehackt zijn... De beheerders kunnen momenteel niet de data op de servers benaderen. Er is nog te weinig bekend om een plan van aanpak te kunnen creëren, het is niet bekend hoe lang het duurt en wat precies de impact is.

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:10	Terugkoppeling contactpersoon over het gesprek.	Analyseren: Overzicht creëren van de data die bij deze cloud leverancier zijn ondergebracht. Overzicht van gekoppelde en afhankelijke systemen (NB: Dit moet dan real-time door iemand aan tafel kunnen worden opgevraagd. Dit moeten ze dan zeker weten uit een live systeem kunnen halen (laptop meenemen) of aangeleverd (voorbereid) worden door de oefenleider.) Beslissen: Beslissen of er moet worden geëscaleerd naar een hoger niveau. Beslissen of het om een security/privacy incident gaat	Contactpersoon en rest van het aanwezige team	

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:20	Cloud leverancier belt met meer info.	Achterhalen: Hoe lang dit duurt Wat de impact is Hoe kan de data vertrouwelijk worden ontvangen van de cloud leverancier?	Accountmanager belt <contactpersoon cloud leverancier>	Hij vertelt dat een hacker volledige toegang tot hun systemen heeft gekregen en alle data gegijzeld heeft. Alle data op alle servers is namelijk versleuteld door ransomware. Gijzelnemer eist geld om het weer vrij te geven. De accountmanager zegt er geruststellend bij dat er gisteravond een backup van de database is geweest. Het kan nog wel lang duren voordat hun cloud omgeving weer in de lucht is maar de organisatie kan haar eigen (ruwe) data wel snel terugkrijgen. Accountmanager cloud leverancier zegt erbij dat er absoluut niet over deze oorzaak gecommuniceerd mag worden onder dreiging van de verstoring van de voortgang/samenwerking.

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14.25	Terugkoppeling contactpersoon over het gesprek	Bespreken: Wat kan de organisatie doen om het bedrijfskritische proces weer op gang te krijgen? Op welke manier kan de data worden ontvangen? Hoe verifiëren we of de data nog integer is? Moeten de juridische zaken en/of privacy officer worden betrokken? Moet er een melding naar het AP worden gemaakt? Hoe kan er vertrouwelijk gecommuniceerd worden met de cloud leverancier? Hoe weten ze dat de contactpersoon is wie hij zegt te zijn? Hoe weten we of de cloud leverancier hard aan het werk is? Weten ze wel wat ze moeten doen? Weten wij wat wij graag willen dat ze gaan doen?	Contactpersoon en rest van het aanwezige team	

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:30	Mensen beginnen te bellen dat ze de dienst niet kunnen benaderen. [Dit zijn voorbeelden. Voor eigen instellingsscenario realistische personen en onderwerpen bedenken.]	Bespreken: Wat gaan we naar wie communiceren? Wat staat er in de contracten met de leverancier? Wie is nu waarvoor verantwoordelijk? Opnieuw contact zoeken met cloud leverancier.	Student(en) Medewerker administratie Onderzoekers	Student: ik kan niet meer bij de laatste versie van mijn scriptie. Deze moet vandaag worden ingeleverd, anders zit ik over de 10 jaar grens en moet ik al mijn studiefinanciering terugbetalen. Ik heb de studentenlijn al gebeld om beklag te doen. Loonadministratie: de verloning moet vandaag plaatsvinden, ik zie opeens geen gegevens meer. Onderzoeker: mijn hele dataset is niet meer beschikbaar. Help!
14.35	Privacy officer belt. Hij wil weten wat de impact is m.b.t. informatiebeveiliging en de gemiste data. En wil weten welke acties we gaan ondernemen.		Privacy officer belt met de prio 1 coördinator.	Privacy officer geeft urgentie en ernst aan. Moet er een melding naar het AP worden gemaakt? Welke exacte data was in het systeem? Hebben we een datamodel? Wie zijn de getroffen personen? Wiens data is gegijzeld? Wat is contractueel afgesproken met de leverancier? Is er een bewerkersovereenkomst?
14.35	(Als er niet is geëscaleerd) Bestuurssecretaris belt op om duidelijkheid te krijgen	Duidelijke update organiseren voor CvB	Bestuurssecretaris belt <persoon in het team met manager functie>	Via twitter/in de wandelgangen heeft een CvB'er lucht gekregen dat alle data weg zijn. Hoe kan dit?! Is de cloud weg? Wat wordt er op dit moment gedaan om dit te fixen en wie is er geïnformeerd?

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:40	Accountmanager belt op		Accountmanager belt <contactpersoon cloud leverancier>	De accountmanager vertelt dat hij goed nieuws heeft, en ook slecht nieuws. Slecht nieuws: de backup stond weliswaar op een andere locatie, maar die was altijd online. De afperser had deze allang weggegooid. Goed nieuws: de code van de cloudomgeving stond nog op de laptop van een ontwikkelaar en de dienst is weer online. De wachtwoorden zijn gereset en de hacker is buiten de deur. De versleutelde database moet helaas als verloren worden beschouwd maar als de organisatie opnieuw de benodigde gegevens kan aanleveren dan zijn ze binnen het uur weer online.
14.45	Terugkoppeling gesprek en overleg	Overleggen: Wat is de alternatief? Wat hebben we zelf om dit proces/systeem opnieuw op te bouwen? Wat is de afweging tussen het stagneren van het kritische bedrijfsproces en alle gegevens opnieuw aan deze partij toe te vertrouwen? Wie kan dat besluit nemen? Zijn er voldoende maatregelen genomen?	Contactpersoon en rest van het aanwezige team	

Tijd	Gebeurtenis	Verwachte acties	Wie	Tekst
14:50	Afronden oefening	Bespreken: Er is enige schade al was het alleen imago en de uren die aan dit incident zijn gespendeerd. Hoeveel is dit? Kunnen we dit ergens verhalen?	Oefenteam	
14.55-15.15	Evaluatie met de aanwezigen		-	-

Bijlage 6 IT Scenario Identiteitsfraude en data integriteit

Casus oefening – Tactisch

Legenda voor aanpassen scenario	
Er staat:	**Te vervangen door:**
Financieel systeem	Willekeurig systeem
CERT-team	Plek waar security meldingen terecht komen
Wachtwoord reset via email	Email forwarding vervangen door inlogpogingen van buitenaf

De servicedesk heeft vandaag een melding ontvangen van Henk, beheerder van het financiële systeem, die de afgelopen dagen regelmatig zijn wachtwoord heeft moeten resetten omdat deze niet meer werkt. Dit is de derde gebruiker die dit in korte tijd meldt. De servicedesk heeft navraag gedaan bij de beheerder van de accounts, deze meldt dat het niet lijkt op een technische storing en heeft het vermoeden dat iemand hier bewust of onbewust aan het rommelen is. De vorige meldingen waren van Annie, een collega van Henk, en Ingrid, een stagiair.

Draaiboek Tactisch scenario

Plaats van de oefening

Bij voorkeur in één ruimte. Ruimte moet voldoende groot zijn om het oefenteam in 2 groepen te kunnen splitsen en separaat aan een deel-opdracht te laten werken. Een break-out ruimte in de buurt kan ook handig zijn.

Start van de oefening

Oefening start op een vooraf aangekondigd moment en plaats. Het oefenteam wordt in deze ruimte bij elkaar geroepen middels een uitnodiging in de agenda. Hier wordt het scenario uitgelegd, waarna de oefening start.

Optioneel: oefening laten starten op een niet aangekondigde moment, waardoor er een extra verassingselement onderdeel wordt van de oefening. Daarmee kan de snelheid van de reactie, maar ook aanwezigheid van key-personen en/of hun vervangers worden getest.

Rollen in het oefenteam	**Rollen in de responscel**
• Afdeling communicatie • IT crisis team • Vertegenwoordiger finance • Functionaris gegevensbescherming	• Servicedesk medewerker • Beheerders financieel systeem (Annie en Henk) • Stagiair HRM (Ingrid) • Politie • AP • Oefenleider • Waarnemer *Als het oefenteam contact wil opnemen met iemand die niet in de responscel zit moet de spelleider deze persoon simuleren of aangeven dat deze persoon niet bereikbaar is.*

Tijd in uren	Gebeurtenis	Verwachte acties	Wie	Tekst
Start ongeplande oefening (oefening waarbij startmoment niet vaststaat, maar start een verassingselement is)				
13:50	Start ongeplande oefening. (oefening waar startmoment niet vaststaat, maar start een verassingselement is). IT Team / CERT escaleert naar voorzitter oefenteam.	Voorzitter oefenteam stemt af met IT Team / CERT en besluit oefenteam bijeen te roepen.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	
Start geplande oefening (oefening waarbij alle deelnemers al in één ruimte zitten)				
14:00	Start geplande oefening. De voorzitter roept het oefenteam bijeen in het crisiscentrum. De voorzitter van het oefenteam vertelt over de crisis en de reden van de bijeenkomst.	De voorzitter geeft briefing over de situatie. De voorzitter vraagt de secretaresse aantekeningen te maken van de taken en acties van het oefenteam.	Voorzitter	De voorzitter leest de casus voor en licht deze toe.
14:05	De servicedesk geeft de melding van de beheerder door aan het CERT team.	Beeldvorming Wat precies het probleem is: Rechten stagiair achterhalen.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Dit is mogelijk een security incident. We weten niet goed wat voor acties er uitgezet moeten worden, of wat voor informatie er beschikbaar is om dit te analyseren. Jullie vast wel, we dragen het incident daarom

				naar jullie over. We horen graag wie ons contactpersoon gaat worden.
14:10	Het oefenteam bedenkt wat ze beschikbaar hebben om een analyse te kunnen maken van het probleem.	Achterhalen: Welke informatie kunnen we opvragen voor analyse? Wat voor acties moeten er worden uitgezet		
14:15	De servicedesk zet een telefoontje door van Henk, functioneel beheerder van het financiële systeem	Blokkeren accounts. Aangifte politie. Bestuur informeren.	Henk belt met teamcoördinator	Hij klaagt dat dit al dagen aan de gang is en vandaag buitengewoon lastig uitkomt. Er gaat iets helemaal mis in het financiële systeem en dit hindert hem in zijn analyse. Drie verschillende klanten hebben geklaagd dat ze hun geld niet hebben ontvangen. Bij het nazoeken is gebleken dat ongeveer 300.000 euro is overgemaakt naar verkeerde rekeningnummers. Henk (zelf) en Annie hebben rechten om dit te muteren. Een collega heeft vandaag een telefoongesprek van Annie opgevangen waarin ze fel discussieerde over rekeningen die ze niet had betaald. Henk gaat uitzoeken wie de data heeft gemuteerd maar vraagt zich af of Annie iets met de accountproblemen te maken kan hebben, wat zijn plausibele scenario's? Wat gaan

				jullie hieraan doen? Wat verwachten jullie van mij?
14:20	Local privacy officer / hoofd HRM belt	Wat kan wel en niet groots worden gecommuniceerd. Welke groepen hebben welke informatie nodig.	Van LPO/HRM aan lid oefenteam op tel. xx xx xx xx xx.	Het log laat zien dat de mutaties onder naam van Henk zijn uitgevoerd. Het lijkt erop dat naast de 3 bedrijven er geen andere gegevens zijn aangepast of geraadpleegd. Bij het raadplegen van de gegevens zijn ook gegevens van de contactpersonen van de drie bedrijven ingezien. Moeten we dit melden bij de 3 bedrijven of de contactpersonen of de AP, of helemaal niet? Wie kunnen we betrekken? Wat vertellen we intern?
14:30	Het bestuur is ingelicht en wil controle	Keuze maken over het offline halen van het systeem. Intern en extern communiceren van deze beslissing.	Voorzitter CvB/RvB / Directeur IT	Bestuur vraagt om advies: Kunnen we vaststellen dat Henk dit heeft gedaan? Moeten we zijn account blokkeren? Met Henk verliezen we het toezicht, moet het systeem uit? Hoe lang dan, dit heeft namelijk enorme consequenties? Moeten we zaken gaan herstellen van een backup? Moeten er nog meer acties worden uitgezet?
	Een servicedesk medewerker belt op	Probleem definiëren als identiteitsfraude. IOC's nazoeken. Nog meer tickets over wachtwoorden via ID	Medewerker servicedesk	Henk belde net (voordat zijn account werd dichtgezet) naar de servicedesk met de mededeling dat bij elke mail die hij ontvangt undeliverable mails van een voor hem onbekend e-mail adres over een volgelopen mailbox op reactie van een mail die hij ontvangen heeft. Ik heb even

		gewijzigd? Procedure wachtwoord wijzigen aanpassen. Waar zijn de mails heen gegaan, is er nog meer daar heen gecommuniceerd? Intern verzoeken om incidenten met wachtwoorden te melden en e-mail forwarding te controleren.		meegekeken en zag dat er een e-mail forwarding op zijn account is ingesteld. Ik dacht dat ik het account van Henk herkende en heb even de ticket historie doorzocht. Een dag of 3 geleden heb ik zijn wachtwoord gewijzigd op zijn eigen verzoek. Henk had zich met een kopie id geïdentificeerd. Ik heb hem net gevraagd of daar misschien iets mis bij is gegaan maar hij zegt dat hij wel veel problemen met zijn account heeft gehad maar nooit een wachtwoord reset heeft aangevraagd.
14:40	Communicatie moet info hebben om statement op te stellen	Helder en feitelijk het probleem verwoorden	Van medewerker communicatie	Kunnen jullie de situatie voor mij in begrijpbare termen samenvatten?
14.45	Mail van e-mail en netwerk beheerder	Nagaan of alle benodigde stappen gezet zijn.	Beheerders	Ook de andere 2 personen hadden mail forwarding aanstaan. Van Annie was op eenzelfde manier als Henk het wachtwoord gewijzigd, de stagiair was waarschijnlijk gewoon een phishing slachtoffer. De aanvaller heeft herhaaldelijk het wachtwoord gewijzigd via de reset link die naar hem door werd gemaild. De e-mail forwardings zijn dichtgezet en we zien spontaan geen nieuwe pogingen meer. Een instelling breed onderzoek naar de IP adressen en e-mail forwarding heeft geen andere zaken gevonden. We zullen het e-mail en IP adres monitoren. De servicedesk

				zal alert blijven. Kunnen we het incident sluiten?
		Optie: tijdsprong: een week later		
14.50	Bestuurslid belt	Doen of aanpassen datalekmelding.	Bestuur	De politie heeft de aangifte serieus genomen, onderzoek naar het IP-adres heeft niets opgeleverd maar er is wel een money mule opgepakt. Het geld is helaas al weg. De identiteitsfraude van Anita is helaas niet beperkt tot de instelling. Ze krijgt boze telefoontjes waarin ze wordt beschuldigd van oplichting op Marktplaats. Nu is ze benaderd door twee collega's die de afgelopen week ook benaderd worden over zaken waar ze niets van af weten. Samen met HRM zijn ze er achter gekomen dat de ID' s die ze via Marktplaats hebben achterhaald dezelfde zijn als die in hun HRM dossier zat. Vermoedelijk zijn de gegevens via het account van de stagiair ontvreemd, hier is geen logging van. Wat kunnen we het beste melden intern/bij AP en welke maatregelen hebben wij getroffen die we kunnen noemen in de melding? Zijn er aan de hand hiervan nog zaken die moeten worden gedaan?
14:55	Afronden oefening	Bespreken:		

15.00-15.30	Evaluatie met de aanwezigen	Hebben we het escalatie proces goed gevolgd? Is met alle stakeholders gecommuniceerd? Zijn we zaken vergeten? Hebben we de informatie die we hebben opgevraagd in het echt ook?	-	-

Bijlage 7 Strategisch scenario Cloudleverancier

Casus oefening – strategisch

Vandaag, [datum], is om [tijdstip] bij de ICT helpdesk van [instelling] de volgende melding van cloudleverancier [leverancier] binnen gekomen.

Een uur geleden is uit de analyse van onze logging gebleken dat een hacker volledig toegang heeft gehad tot onze systemen, waaronder de systemen van [instelling]. Hoe lang deze hack al aan de gang is, is op dit moment onduidelijk. Ook is niet bekend welke acties de hacker heeft uitgevoerd en welke gegevens hierbij zijn geraakt. Onderzoek hiernaar is in gang gezet. Wij houden u op de hoogte van de voortgang en uitkomsten van dit onderzoek.

De omvang van dit cyberincident en de consequenties voor de continuïteit van de bedrijfsprocessen van de instelling zijn zodanig dat het oefenteam om [tijdstip] bijeen geroepen is in vergaderruimte [ruimte].

Het Oefenteam [instelling] bestaat uit de volgende functionarissen:

- Xxx
- Xxx
- Xxx
-

Draaiboek Strategisch scenario

Plaats van de oefening

Bij voorkeur in één ruimte. Ruimte moet voldoende groot zijn om het oefenteam in 2 groepen te kunnen splitsen en separaat aan een deel-opdracht te laten werken. Een break-out ruimte in de buurt kan ook handig zijn.

Start van de oefening

Oefening start op een vooraf aangekondigd moment en plaats. Het oefenteam wordt in deze ruimte bij elkaar geroepen middels een uitnodiging in de agenda. Hier wordt het scenario uitgelegd, waarna de oefening start.

Optioneel: oefening laten starten op een niet aangekondigde moment, waardoor er een extra verassingselement onderdeel wordt van de oefening. Daarmee kan de snelheid van de reactie, maar ook aanwezigheid van key-personen en/of hun vervangers worden getest.

Rollen in het oefenteam	**Rollen in de responscel**
• Lid RvB/CvB • Secretaris/notulist • Afdeling communicatie • Hoofd IT • Vertegenwoordiger business/themadirecteur/faculteitsdirecteur • Crisiscoördinator • …	• IT team/CERT (belangrijke rol) • Communicatiemedewerker • Journalist • Decaan instituut • Jurist • Spelleider • Waarnemer *Als het oefenteam contact wil opnemen met iemand die niet in de responscel zit moet de spelleider deze persoon simuleren of aangeven dat deze persoon niet bereikbaar is.*

Tijd in uren	Gebeurtenis	Verwachte acties	Wie	Tekst
Start ongeplande oefening (oefening waarbij startmoment niet vaststaat, maar start een verassingselement is)				
13:50	Start ongeplande oefening. (oefening waar startmoment niet vaststaat, maar start een verassingselement is). IT Team / CERT escaleert naar voorzitter oefenteam.	Voorzitter oefenteam stemt af met IT Team / CERT en besluit oefenteam bijeen te roepen.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Vandaag, [datum], is om [tijdstip] bij de ICT helpdesk van [instelling] de volgende melding van cloudleverancier [leverancier] binnen gekomen. *Een uur geleden is uit de analyse van onze logging gebleken dat een hacker volledig toegang heeft gehad tot onze systemen, waaronder de systemen van [instelling]. Hoe lang deze hack al aan de gang is, is op dit moment onduidelijk. Ook is niet bekend welke acties de hacker heeft uitgevoerd en welke gegevens hierbij zijn geraakt. Onderzoek hiernaar is in gang gezet. Wij houden u op de hoogte van de voortgang en uitkomsten van dit onderzoek.* Ik stel voor dat we het oefenteam bij elkaar roepen. Ben jij het hiermee eens?
Start geplande oefening (oefening waarbij alle deelnemers al in één ruimte zitten)				

14:00	Start geplande oefening. De voorzitter roept het oefenteam bijeen in het crisiscentrum. De voorzitter van het oefenteam vertelt over de crisis en de reden van de bijeenkomst.	De voorzitter geeft briefing over de situatie. De voorzitter vraagt de secretaresse aantekeningen te maken van de taken en acties van het oefenteam.	Voorzitter	De voorzitter leest de casus voor en licht deze toe.
14:05	Het IT team / CERT meldt zich telefonisch bij het oefenteam.	Achterhalen: Wat precies het probleem is: welke data zijn precies gehackt? Wat hieraan kan worden gedaan Hoe lang dit gaat duren	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Wij zijn zojuist door de ICT helpdesk gebeld met de melding van de cloudleverancier. Wij zullen met hen contact opnemen om de volgende zaken te achterhalen: Welke gegevens van ons zijn geraakt Hoe lang is de hacker al op het systeem Identiteit van de hacker Oorzaak van de hack Genomen maatregelen Hebben jullie nog andere vragen voor de cloudleverancier?
14:10	Het oefenteam maakt een inschatting van de omvang van het incident en de gevolgen voor de organisatie	Achterhalen: Is de hack al bekend buiten de instelling?		

		Zijn er data gelekt? Melding maken bij AP?		
14:15	Het IT team / CERT meldt zich opnieuw telefonisch bij het oefenteam.	Keuze maken over het off-line halen van het systeem. Intern en extern communiceren van deze beslissing.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	We hebben contact gehad met de cloudleverancier. Nog niet veel nieuwe informatie ontvangen, maar wel een vraag. Vanwege de onduidelijkheid van de situatie stelt de cloudleverancier het systeem off-line te halen. Kunnen wij hiermee instemmen?
14.20	Communicatieafdeling meldt dat op twitter berichten langskomen van onderzoekers/ patiënten/medewerkers/ studenten	Besluiten: Wat communiceren wij intern en extern?	Van communicatiemedewerker aan Hoofd Communicatie op tel. xx xx xx xx xx.	Via onze media watching zien wij de volgende berichten voorbij komen: *Student: ik kan niet meer bij de laatste versie van mijn scriptie. Deze moet vandaag worden ingeleverd, anders zit ik over de 10 jaar grens en moet ik al mijn stufi terugbetalen. Ik heb de studentenlijn al gebeld om beklag te doen.* *Loonadministratie: de verloning moet vandaag plaatsvinden, ik zie opeens geen gegevens meer.*

				Onderzoeker: mijn hele dataset is niet meer beschikbaar. Help! Ik stel voor dat wij intern en extern communiceren over het incident. Is het oefenteam hiermee akkoord en kunnen we afstemmen over de inhoud van het persbericht?
14:25	Het IT team / CERT meldt zich opnieuw telefonisch bij het oefenteam.	Bepalen van vervolgstappen, waaronder resetten van wachtwoorden van gebruikers.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	We hebben opnieuw contact gehad met de cloudleverancier en de volgende informatie ontvangen: Uit forensische analyse blijkt dat de hacker al twee weken op het systeem aanwezig is. De hacker heeft intensief gegeven gedownload, waaronder de volgende gegevens van onze instelling: [studentgegevens] [personeelsgegevens] [patiëntgegevens] [onderzoeksgegevens].

				Het is niet uitgesloten dat de hacker ook wachtwoorden van onze gebruikers heeft achterhaald. De oorzaak lag in twee zaken: Verkeerde instellingen van certificaten (weak ciphers). Achterstallig onderhoud (belangrijk patch op de server is gemist). De cloudleverancier voert herstelwerkzaamheden uit die morgen aan het einde van de dag zijn afgerond.
14:30	Journalist belt met vraag om een statement.	Geen commentaar	Van journalist aan lid oefenteam op tel. xx xx xx xx xx.	Met xxx van het Algemeen Dagblad. Cloudleverancier X heeft een persbericht uitgedaan dat zij vanochtend gehackt zijn. Jullie zijn klant van deze leverancier staat op hun site. Wij zien berichten over dit incident aan jullie instelling gerelateerd op social media voorbij komen. Wat is er precies bij jullie instelling aan de hand?
14:35	Decaan nieuw opgericht internationaal instituut neemt contact op	Besluiten of contact moet worden opgenomen met partneruniversiteiten. Wat wordt aan hen gecommuniceerd?	Van decaan aan lid oefenteam op tel. xx xx xx xx xx.	Het blijkt dat er ook gegevens van studenten van partneruniversiteiten in de cloud zaten. Moeten deze partners worden ingelicht?

14:40	Het IT team / CERT meldt zich opnieuw telefonisch bij het oefenteam.	Bepalen van vervolgstappen.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Wij hebben een melding van het NCSC ontvangen dat omvangrijke hoeveelheden gegevens van onze instelling op pastebin zijn geplaatst. Wij hebben dit geverifieerd en dit klopt. Er staan ook inloggegevens en wachtwoorden van [xxx] gebruikers van ons bij.
14.45	Tweakers.net publiceert een stuk over de enorme hack op cloud leverancier.	Bepalen van vervolgstappen.	Van communicatiemedewerker aan Hoofd Communicatie op tel. xx xx xx xx xx.	Ik wil je graag wijzen op het volgende artikel op de website Tweakers.net.
14.50	Juridische Zaken meldt zich telefonisch voor overleg.	Afstemming over aangifte en melding datalek. Ook moet de aansprakelijkheid van de leverancier worden besproken.	Van Juridische Zaken aan voorzitter oefenteam op tel. xx xx xx xx xx.	Met Juridische Zaken. Wij willen graag overleg inzake het incident voor het doen van aangifte en met melden van een datalek bij de Autoriteit Persoonsgegevens. Ook willen we de leverancier aansprakelijk stellen. Wanneer en hoe kunnen we hierover overleggen.
14:55	Afronden oefening	Bespreken: Er is enige schade al was het alleen imago en de uren die aan dit incident zijn gespendeerd. Hoeveel is dit? Kunnen we dit ergens verhalen?		

15.00-15.30	Evaluatie met de aanwezigen	-	-	-

Bijlage 8 Strategisch scenario Identiteitsfraude en data integriteit

Casus oefening – strategisch

Gisteren, [datum], is gebleken dat het HRM systeem van [instelling] enige tijd geleden is gehackt, waarbij iemand [paspoortkopieën/BSN] uit het systeem heeft weten te halen. Deze gegevens zijn gebruikt om accounts over te nemen van [systeembeheerders/mensen met hoog financieel mandaat]. Hiermee zijn in de afgelopen weken [in ieder geval 300.000 euro aan incorrecte overboekingen gemaakt/in ieder geval 100 gegevens in het studentvolgsysteem aangepast/een hoeveelheid data in een database voor een zeer groot onderzoek aangepast]. Op dit moment is het nog onduidelijk hoeveel data precies is gemanipuleerd.

De omvang van dit cyberincident en de consequenties voor de continuïteit van de bedrijfsprocessen van de instelling zijn zodanig dat het oefenteam om [tijdstip] bijeen geroepen is in vergaderruimte [ruimte].

Het Oefenteam [instelling] bestaat uit de volgende functionarissen:

- Xxx
- Xxx
- Xxx
-

Draaiboek Strategisch scenario

Plaats van de oefening

Bij voorkeur in één ruimte. Ruimte moet voldoende groot zijn om het oefenteam in 2 groepen te kunnen splitsen en separaat aan een deel-opdracht te laten werken. Een break-out ruimte in de buurt kan ook handig zijn.

Start van de oefening

Oefening start op een vooraf aangekondigd moment en plaats. Het oefenteam wordt in deze ruimte bij elkaar geroepen middels een uitnodiging in de agenda. Hier wordt het scenario uitgelegd, waarna de oefening start.

Optioneel: oefening laten starten op een niet aangekondigde moment, waardoor er een extra verassingselement onderdeel wordt van de oefening. Daarmee kan de snelheid van de reactie, maar ook aanwezigheid van key-personen en/of hun vervangers worden getest.

Rollen in het oefenteam	**Rollen in de responscel**
• Lid RvB/CvB • Secretaris/notulist • Afdeling communicatie • Hoofd IT • Vertegenwoordiger business/themadirecteur/faculteitsdirecteur • Crisiscoördinator • …	• IT team/CERT (belangrijke rol) • Communicatiemedewerker • Journalist • HRM medewerker • Jurist • Oefenleider • Waarnemer *Als het oefenteam contact wil opnemen met iemand die niet in de responscel zit moet de spelleider deze persoon simuleren of aangeven dat deze persoon niet bereikbaar is.*

Tijd in uren	Gebeurtenis	Verwachte acties	Wie	Tekst
Start ongeplande oefening (oefening waarbij startmoment niet vaststaat, maar start een verassingselement is)				
13:50	Start ongeplande oefening. (oefening waar startmoment niet vaststaat, maar start een verassingselement is). IT Team / CERT escaleert naar voorzitter oefenteam.	Voorzitter oefenteam stemt af met IT Team / CERT en besluit oefenteam bijeen te roepen.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Gisteren, [datum], is gebleken dat het HRM systeem van [instelling] enige tijd geleden is gehackt, waarbij iemand [paspoortkopieën/BSN] uit het systeem heeft weten te halen. Deze gegevens zijn gebruikt om accounts over te nemen van [systeembeheerders/mensen met hoog financieel mandaat]. Hiermee zijn in de afgelopen weken [in ieder geval 300.000 euro aan incorrecte overboekingen gemaakt/in ieder geval 100 gegevens in het studentvolgsysteem aangepast/een nog vast te stellen hoeveelheid data in een database voor een zeer groot onderzoek aangepast]. Op dit moment is het nog onduidelijk hoeveel data precies is gemanipuleerd. Ik stel voor dat we het oefenteam bij elkaar roepen. Ben jij het hiermee eens?
Start geplande oefening (oefening waarbij alle deelnemers al in één ruimte zitten)				

14:00	Start geplande oefening. De voorzitter roept het oefenteam bijeen in het crisiscentrum. De voorzitter van het oefenteam vertelt over de crisis en de reden van de bijeenkomst.	De voorzitter geeft briefing over de situatie. De voorzitter vraagt de secretaresse aantekeningen te maken van de taken en acties van het oefenteam.	Voorzitter	De voorzitter leest de casus voor en licht deze toe.
14:05	Het IT team / CERT meldt zich telefonisch bij het oefenteam.	Achterhalen: Wat precies het probleem is: welke systemen zijn precies gehackt en wat is er aangepast? Wat hieraan kan worden gedaan Hoe lang dit gaat duren	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	Wij hebben vastgesteld dat in ieder geval de accounts van de volgende mensen zijn overgenomen: […., …., …., …]. Deze accounts zijn ondertussen dicht gezet om verdere malafide praktijken te voorkomen. Op dit moment zijn we verder aan het uitzoeken hoeveel wijzigingen zijn gemaakt in [gekozen systeem of database].
14:10	Het oefenteam maakt een inschatting van de omvang van het incident en de gevolgen voor de organisatie	Achterhalen: Is de hack al bekend buiten de instelling? Zijn er data gelekt? Melding maken bij AP? Wat zijn de mogelijke scenario’s en hoe kunnen deze het best worden voorkomen/afgehandeld?		

14:15	Het IT team / CERT meldt zich opnieuw telefonisch bij het oefenteam.	Keuze maken over het off-line halen van het systeem. Intern en extern communiceren van deze beslissing.	Van IT team / CERT aan voorzitter oefenteam op tel. xx xx xx xx xx.	We kunnen op dit moment niet vaststellen of er nog andere gecompromitteerde accounts zijn en of er nog wijzigingen worden gedaan die niet kloppen. Wij stellen daarom voor om het systeem off-line te halen tot duidelijk is hoe groot het probleem precies is. Zijn jullie hiermee akkoord?
14:20	HRM belt om te informeren wat aan de medewerkers kan worden gemeld over de identiteitsfraude.	Wat kan wel en niet groots worden gecommuniceerd. Welke groepen hebben welke informatie nodig	Van HRM aan lid oefenteam op tel. xx xx xx xx xx.	Op de werkvloer zijn nu een aantal mensen ingelicht over de identiteitsfraude, maar een groot deel van de medewerkers is niet officieel op de hoogte. Men begint nu onrustig te worden en er gaan allemaal vreemde verhalen de ronde. Wat kunnen we aan iedereen communiceren?
Optie: tijdsprong: een week later				
14:30	Het IT team/CERT geeft een update wat er de afgelopen dagen is gevonden	Keuze maken tussen nog langer het systeem onbereikbaar houden of terugzetten naar een eerdere versie. Bepalen wat de impact is van de verschillende opties voor het primaire proces/vitale bedrijfsproces? Wat betekent dit voor de verschillende stakeholders?		Ondertussen is vastgesteld dat de hoeveelheid overgenomen accounts veel groter is dan eerst gedacht. Alle accounts zijn daarom ondertussen gereset en de verificatie methode is zo aangepast dat daar niet met gestolen paspoortkopieën mee kan worden gesjoemeld. Wat er allemaal is aangepast in [het systeem] is echter nog steeds niet duidelijk. Naar onze inschatting hebben we nog minstens een week nodig om dat na te gaan, waarbij de kans aanwezig is dat het dan nog steeds niet helemaal

		Wat is de impact op de reputatie van de instelling?		duidelijk is. Een alternatief is om een backup van [kies een ongemakkelijk lange tijd geleden] te gebruiken. Dit zou betekenen dat [beschrijf de impact voor het financiële proces/ander primair proces wat samenhangt met dit systeem]. Wat willen jullie dat we doen?
14:40	Journalist belt met vraag om een statement over integriteit data.	Als het nog niet eerder is besloten: wat is het officiële statement naar buiten?	Van journalist aan lid oefenteam op tel. xx xx xx xx xx.	Met [journalist van de Gelderlander/ander lokaal blad]. Er zijn geruchten dat jullie zijn gehackt. Is dit inderdaad het geval? Welke systemen zijn geraakt?
14.45	HRM meldt dat de gestolen paspoortkopieën terug zijn te vinden op marktplaats	Besluiten: Wat communiceren wij intern en extern? Is er al aangifte gedaan? Hoe kan het gevoel van veiligheid voor medewerkers worden hersteld?	Van communicatiemedewerker aan Hoofd Communicatie op tel. xx xx xx xx xx.	We hebben een aantal meldingen gekregen dat de gestolen paspoortkopieën terug te vinden zijn op marktplaats, wat bij nadere inspectie bleek te kloppen. Marktplaats is ingelicht en zal de advertenties verwijderen, maar kan niet voorkomen dat dit vaker voor gaat komen. Van de vertrouwenspersoon krijgen wij steeds meer signalen dat medewerkers zich niet veilig voelen door hoe met hun gegevens wordt omgegaan.
14.50	Juridische zaken belt om af te stemmen over aanpassen datalekmelding.	Bepalen aanpassen datalekmelding.	Van Juridische zaken aan lid oefenteam op tel. xx xx xx xx xx.	De melding die we vorige week aan de AP hebben gedaan ging om een relatief klein datalek, maar ondertussen lijkt het een stuk groter te zijn. Wat kunnen we het beste melden en welke maatregelen hebben wij getroffen die we kunnen noemen in de melding?

14:55	Afronden oefening	Bespreken: Er is enige schade al was het alleen imago en de uren die aan dit incident zijn gespendeerd. Hoeveel is dit? Kunnen we dit ergens verhalen?		
15.00-15.30	Evaluatie met de aanwezigen	-	-	-

Dankwoord

Deze handleiding en de bijbehorende voorbeeldscenario's zijn gemaakt met medewerking van:

Raoul Vernede (Universiteit Wageningen)

Anita Polderdijk-Rijntjes (Hogeschool Windesheim)

Remon Klein Tank (Universiteit Wageningen)

Jan Willem Schoemaker (ErasmusMC)

Mladen Acinger (Erasmus Universiteit)

Peter Peters (Universiteit Twente)

Albert Hankel (SURFnet)

Jacco Blom (Universiteit Utrecht)

Claartje Uitterhoeve (Graafschap College)

Jan Wiss (Hogeschool Inholland)

Sebas Daniels (Hogeschool Fontys)