|  |
| --- |
| Gezamenlijke oefening  (OTO Oefening) |
|  |
| Proces oefening |
|  |
| Voor intern gebruik |

# Doel van de oefening

Het doel van deze OTO-sessie is het oefenen van de processen en interacties tussen een interne Security-afdeling en een CERT. Hierbij is wederzijds begrip en inzicht in elkaars processen en jargon cruciaal om de oefening succesvol af te ronden. **Deze training betreft een fictief, maar realistisch scenario**, waarbij een aantal verschillende mijlpalen moeten worden behaald en onderbrekingen kunnen worden gegeven vanuit de ‘spelleiders’. Deze oefening zal wellicht aanpassingen vereisen aan de afdelings- en/of functienamen om inzetbaar te zijn voor een andere organisatie.

Deze training is bijzonder effectief en inzichtgevend voor (nieuwe) medewerkers bij dergelijke afdelingen, mits de deelnemers zich houden aan de beschreven spelregels, met name in het duidelijk beschrijven en onderbouwen van beslissingen en processen naar alle andere deelnemers.

# Vereisten

* Schrijfartikelen (voor notities)
* Laptop
* Per locatie één ruimte
* Tijdsbesteding: 2 uur – max. 1 uur uitleg en uitvoering, max. 1 uur evaluatie
* Conference call (bv. via ‘spin’) tussen de twee locaties:

## Opzet

* Twee spelleiders, ieder uit de verschillende afdelingen, die zowel de inhoudelijke als procesbewakingsrol kunnen vervullen
* Deelnemers vervullen hun reguliere rol (Security dan wel CERT)
* Optioneel: onafhankelijke ‘monitor’ door non-Security / non-CERT collega

## Spelregels

* Beslissingen/acties moeten worden bereikt via groepsconsensus. Deze moeten worden onderbouwd aan de spelleider(s)
* De spelleiders kunnen een Interrupt geven met aanvullende informatie en/of vragen.
* Maak gebruik van de Wiki’s en vergelijkbare documentsystemen
* Bij gelijktijdig overleg wordt gebruik gemaakt van de ‘Mute’-functie van de ‘spin’

# Beschrijving

## Rollen

* 1+ Security afdeling **(SA)**
* 1+ CERT **(CERT)**
* 1+ Integriteitsconsultant(s) **(IC)**
* 1+ Analist(en) **(AN)**
* 0+ Fraude-afdeling **(FA)** (passieve rol)
* 0+ Compliance **(CO)** (passieve rol)

## Trigger

Een klokkenluider meldt een integriteitskwestie. Hij heeft gezien dat een directe collega, ‘Bernadette Mollema-Jansen’ **(fictieve naam, afkorting BMJ)**, continu klantgegevens lijkt te kopiëren en plakken uit een klantsysteem naar een Excel-bestand. De melder denkt dat het al om honderden klanten gaat.

## Docentenhandleiding

### Algemene vereisten

* Verslaglegging in Security- en CERT-systemen
* Threat Intel, indien beschikbaar/aanwezig in de organisatie
* Bijhouden rapportage(s)

### Volledig uitgewerkt stappenplan van de oefening:

1. SA voert de melding in hun systemen
2. *SA voert de melding in als ‘integriteitszaak’, omdat het hier een klokkenluidersmelding gaat. Dit zijn meldingen die directe actie vereisen.*
3. SA overlegt met management over de toewijzing van IC aan deze case
   1. **Interrupt: potentiële melding datalek bij Autoriteit Persoonsgegevens (CO)**
4. IC *is verantwoordelijk voor verdere behandeling van het incident en is de ‘lead investigator’*
5. IC laat nakijken tot welke systemen BMJ toegang heeft
   1. IC *resultaat: BMJ heeft onder andere toegang tot systemen met klantdata!*
6. IC laat navraag doen bij de klokkenluider over BMJ: in welk systeem zouden de opvragingen hebben plaatsgevonden, wat is de standplaats van BMJ, en is er andere relevante informatie beschikbaar?
   1. IC *resultaat: idem 5a, standplaats blijkt ‘lokatie A’*
7. IC geeft opdracht aan SA voor opvragen van de email en homedirectory van BMJ
   1. IC *resultaat: levert email en homedirectory op*
   2. IC geeft opdracht tot onderzoek van deze gegevens
8. IC geeft opdracht logging uit de klantsystemen aan te leveren
9. IC geeft AN opdracht de logfiles uit de klantsystemen onderzoeken
   1. AN *resultaat: logfile toont bevraagde klanten*
   2. AN *resultaat: subset van bevraagde klanten wordt herkend als klanten waar meldingen zijn van ontvangen*
10. AN stelt hulpvraag aan digitaal forensische onderzoekers van CERT om logging te onderzoeken. Deze hulpvraag aan CERT van IC heeft urgentie!
    1. CERT *resultaat: inlogpogingen worden getraceerd tot één IP-adres op lokatie A (terugkoppeling via bijvoorbeeld CERT  AN  IC)*
11. IC informeert en overlegt met FA of er overeenkomsten zijn met onderzoeken
    1. IC *resultaat: FA heeft opgemerkt dat er veel klantmeldingen zijn geweest, waarbij het merendeel uit lokatie A of de omgeving kwam. Koppeling 9b: het blijkt dat veel van deze meldingen overeenkomen met de subset van klanten uit 9b*
12. **Interrupt:** AN meldt, na eigen onderzoek dat er geen relevante gegevens (klantdata, e-mails, Excelbestanden) zijn te vinden in de email of de homedirectory,
13. IC stelt hulpvraag aan CERT om forensisch onderzoek te laten doen naar de werkplek/laptop van BMJ. Dit is wederom een urgentie kwestie.
14. *CERT verricht de forensische inbeslagname van de werkplek en materialen in overleg/samenwerking met IC en evt. bewaking*
15. CERT maakt een forensisch integere kopie (image) van de laptop en onderzoekt deze
    1. *CERT resultaat: data-/metacarving levert verwijderde Excel-bestanden en e-mails op, met daarin klantgegevens die zijn verstuurd naar een enkel email-adres, wat weer kan worden gekoppeld aan een gebruiker op lokatie A*
    2. ***Interrupt: definitieve bevestiging datalek AP (CO)***
16. **Interrupt deadline: Threat Intel voor CERT (indien aanwezig/beschikbaar)**
17. CERT levert onderzoeksrapport op aan IC
18. IC *resultaat: klant in lokatie A, IP-adres inlogpogingen, Threat Intel etc., zijn allemaal herleidbaar naar hetzelfde adres. BMJ heeft klantgegevens opgezocht in de klantsystemen en verstuurd aan een onbekende contactpersoon op lokatie A*
19. **Interrupt deadline: ROI (‘raadpleging open internetbronnen’ onderzoek) door IC/AN**
20. IC/AN *resultaat: ROI onderzoek naar relatie tussen BMJ en ‘klant lokatie A’*
21. IC handelt onderzoek af
    1. zoekt contact met de manager van de manager van BMJ
    2. IC *resultaat: interview BMJ*
    3. IC maakt rapport op en draagt dit over aan afdeling HR (ontslag medewerker, verhaal kosten e.d.)

