TLP:GREEN

IR-5 TABLETOP-OEFENINGEN

Incident Response - Incident Response Readiness

Best Practice versie 1.1

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supply chain, netwerken, systemen en (gevoelige) informatie. Daarnaast hebben moderne organisaties die veel informatie verwerken een grote afhankelijkheid van digitalisering. Dat maakt dat deze organisaties kwetsbaar zijn voor verstoringen in de keten.

Om de gevolgen van cyberincidenten te beperken, is het van belang om Incident Response ingericht te hebben. Incident Response gaat over het vermogen, de processen, tools en technologieën van een organisatie die nodig zijn om te reageren op cyberdreigingen, -incidenten of -aanvallen. Het doel van Incident Response is dat de bedrijfsvoering zo min mogelijk wordt verstoord tijdens een cyberincident.

Incident Response gericht op cyberincidenten kent een aantal specifieke kenmerken en processtappen ten opzichte van regulier incidentmanagement. Regulier incidentmanagement richt zich primair op gebruikerservaring en het zo snel mogelijk oplossen van storingen om tot een optimale gebruikersbeleving te komen. Incident Response in de context van cyberincidenten richt zich op bedrijfsprocessen als geheel en het voorkomen van (verdere) schade. Incident Response in de context van cyberincidenten geeft daarom ook veel aandacht aan risicobeperkende maatregelen die uitbreiding van het beveiligingsincident – en daarmee vervolgschade - voorkomen. Deze elementen zijn in regulier incidentmanagement vaak niet of onvoldoende aanwezig.

Het programma Versterken SOC Stelsel Rijk heeft diverse producten ontwikkeld die organisaties kunnen gebruiken bij het inrichten c.q. optimaliseren van Incident Response. Dit document bevat handvatten waarmee een organisatie stapsgewijs het Incident Response kan inrichten c.q. optimaliseren.

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. Dit document maakt onderdeel uit van een tiental miniproducten die rijksorganisaties helpt om een aantal operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor IT-management, IT auditor, (Security) Incidentmanager, Informatie Security Manager, CISO, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	2-7-2025	Initiële versie
V1.1	2-7-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Incident Response – Tabletop Begeleidershandboek	Zie "IR-5, Incident Response – Tabletop Begeleidershandboek" onder Incident Response Readiness
Incidente Response - Procesmodel	Zie "IR-4, Incident Response – Procesmodel" onder Incident Response Readiness
Incident Response miniproducten	Zie Incident Response Readiness van VSSR
Baseline Informatiebeveiliging Overheid v1.04zv	https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf
Woordenboek Cyberveilig Nederland	Woordenboek - Cyberveilig Nederland
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Definitie	Toelichting
Tabletop oefening	Een tabletop oefening is een gesimuleerde situatie (incident) dat in een vergaderruimte of online setting wordt besproken. De deelnemers reageren (response) op een fictief incident alsof het echt gebeurt.

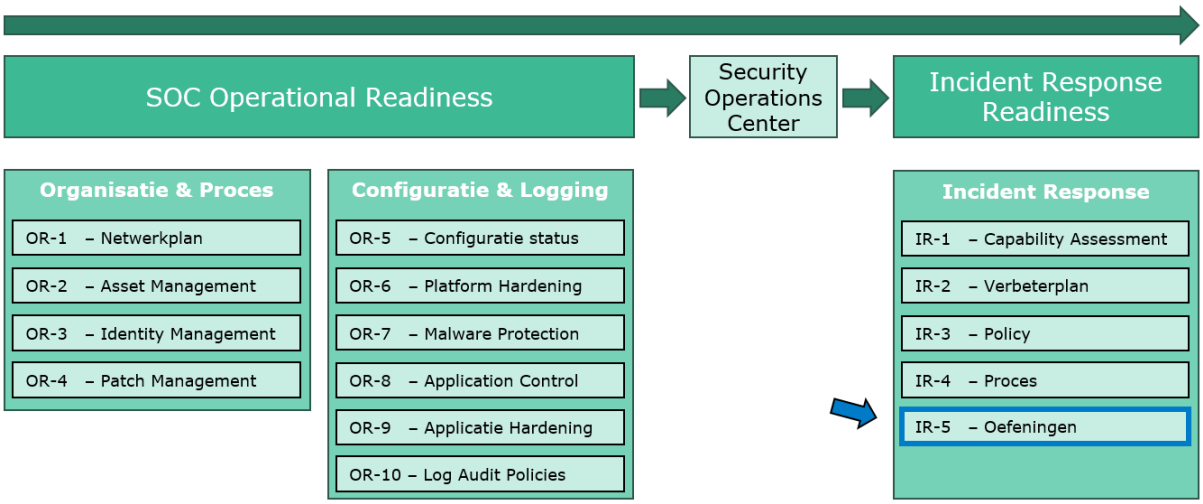
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de Incident Response Readiness **miniproducten**. De Incident Response Readiness miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). We speken over miniproducten omdat de producten compact en overzichtelijk zijn waardoor organisaties in korte tijd en met behapbare hoeveelheden werk progressie kunnen maken. De producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC securitymelding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Incident Response** in het VSSR-miniproducten-raamwerk.



Figuur 1: Dit document als onderdeel van het VSSR-miniproducten raamwerk

De documenten onder IR-5 Oefeningen bestaan uit:

- Tabletop-oefeningen (**Dit document**)
  PDF document voorziet in verschillende tabletop-oefeningen.

- Tabletop begeleidershandboek
  PDF document waarin ondersteunende acties voor begeleider en/of facilitator worden beschreven.

3 Leeswijzer

Deze leeswijzer helpt je bij het effectief gebruiken van dit document en het correct toepassen van de tabletop-oefeningen.

3.1 Doel van dit document (Tabletop-oefeningen)

Dit document helpt organisaties om Incident Response processen en procedures te testen, verbeterpunten te signaleren en teams te laten oefenen in het effectief samenwerken en onder druk beslissingen nemen. Op deze wijze bouwen teams ervaring en routine op in het afhandelen van cyberincidenten. Door regelmatig tabletops-oefeningen uit te voeren zijn organisaties beter voorbereid om effectief en adequaat te reageren op beveiligingsincidenten.

Ter ondersteuning van tabletop-begeleider en -facilitator is er ook een tabletop-begeleidershandboek beschikbaar (zie "Incident Response – Tabletop Begeleidershandboek (IR-5)".

3.2 Opbouw van het document

Dit document bestaat uit een voorwoord en inleiding die de noodzaak van effectieve incidentresponse in de huidige digitale omgeving beschrijft. Hier worden de algemene doelstellingen van de tabletop-oefeningen geïntroduceerd, evenals de opzet en structuur van de oefeningen. Deze sectie vormt de basis voor het begrijpen van de specifieke oefeningen die volgen.

In hoofdstuk 5 is de generieke opzet van tabletop-oefeningen beschreven. Daarna worden de processtappen voor incidentoplossing uitgelegd en de verantwoordelijkheden van betrokkenen verduidelijkt.

Hoofdstuk 6 gaat in op de scenario keuzes en introduceert het dobbelsteenspel voor scenariokeuze. Het dobbelsteensysteem is een speelse manier om willekeurige incidenten en assets te kiezen.

In dit hoofdstuk worden ook drie voorbeelden van tabletop-scenario's geïntroduceerd:

I. de Informatiebeveiligingsmeldinguitloop (uitgewerkt is in hoofdstuk 7);
II. de Beveiligingsincidentuitloop (uitgewerkt in hoofdstuk 8);
III. de Crisis-escalatieoefening (uitgewerkt in hoofdstuk 9).

Elk scenario heeft, naast de eerder geïntroduceerde algemene doelstellingen, zijn eigen doelstellingen, deelnemers, agenda en benodigde hulpbronnen.

Aan het einde van dit hoofdstuk worden er nog een aantal praktische handvatten gegeven die helpen om het beschreven raamwerk concreet toe te passen.

In de hoofdstukken 7, 8 en 9 zijn de drie voorbeelden van oefenscenario's uitgewerkt. Elke tabletop-oefening is aan de hand van een drietal fases uitgewerkt. De voorbereidende fase beschrijft de acties die nodig zijn om een tabletop-oefening voor te bereiden. Vervolgens wordt de uitvoerende fase beschreven en als laatste de evaluatie en nazorg die noodzakelijk is na afronding van de tabletop-oefening.

De processtappen voor incidentoplossing worden per scenario in detail besproken, waarbij de voorbereiding, registratie, classificatie, onderzoek, containment, oplossing en evaluatie worden behandeld. Deze stappen zijn generiek onderdeel van het incidentresponseproces en worden dus per scenario herhaald en toegepast in de oefeningen.

4 Inleiding

In de hedendaagse digitale wereld is een effectieve afhandeling van beveiligingsincidenten essentieel voor het waarborgen van de digitale weerbaarheid van organisaties. Beveiligingsincidenten zoals datalekken, hack-aanvallen of ransomware-aanvallen treden onverwachts op en vereisen een snelle, goed gecoördineerde reactie om de schade te beperken, het herstel te versnellen en vast te stellen wat er precies wanneer is gebeurt. Dit document richt zich op drie tabletop-oefeningen die zijn ontworpen om de incidentresponse binnen de organisatie te versterken en de paraatheid van het team te vergroten. Daarmee is het gericht op het incidentmanagement en -responseteam en de directe belanghebbenden hieromheen.

Tijdens een tabletop-oefening worden aspecten van het incidentresponseproces doorlopen. De begeleider of facilitator heeft van tevoren de informatie over het gesimuleerde beveiligingsincident en over de rollen van de spelers. Tijdens de oefening reageren de spelers op in het scenario opgezette gebeurtenissen.

Door het doorlopen van alle stappen uit het incident responseproces wordt inzichtelijk of het proces effectief gevolgd kan worden, de processtappen goed uitvoerbaarzijn, de benodigde informatie beschikbaar is en of het mogelijk is effectieve besluitvorming te krijgen over de keuzes die in dit proces gemaakt moeten worden.

Het incidentresponseteam kan daarnaast met de tabletop relevante informatie delen, overzicht krijgen en (adequate besluiten en communicatie) maatregelen nemen. Het is een goede optie als men in relatieve rust de incidentresponse en de onderlinge samenwerking wil oefenen en/of specifieke vaardigheden wil trainen.

De oefeningen zijn opgebouwd rondom verschillende fasen van een incidentafhandeling, van de eerste informatiebeveiligingsmelding tot de uitloop van een daadwerkelijk incident en uiteindelijk de escalatie naar een crisis. Door middel van realistische scenario's wordt het team geoefend om effectief samen te werken, beslissingen te nemen onder druk en hun reacties in een gecontroleerde en veilige omgeving te testen. De oefeningen zullen niet alleen de samenwerking en communicatie binnen het team verbeteren, maar ook helpen om de algehele incidentresponse te optimaliseren. Dit kan voor zowel het proces als de specifieke opgezette incidentresponseplannen, ook wel “play books” genoemd.

Dit document biedt een overzicht van de opzet van de oefeningen, de betrokken rollen en de mogelijke doelstellingen die behaald kunnen worden. Dit is het raamwerk van de tabletop-oefeningen. Naast de “spelers” in de tabletop oefening zijn er ook beknopte aanwijzingen opgenomen voor begeleiders of facilitators van de oefeningen zodat het maximale resultaat van de oefening gerealiseerd kan worden. Daarnaast is er voor hen ook een separaat document waar uitgebreid op de beveleiding en facilitering wordt ingegaan.

4.1 Doelstellingen

De mogelijke doelstellingen van deze tabletop-oefeningen zijn veelzijdig. Het zijn oefeningen die uiteindelijk helpen in het versterken van de digitale weerbaarheid binnen de organisatie. De eerder geïntroduceerde hoofddoelstellingen waren:

- Het valideren van de beschikbaarheid en juistheid van de procesdocumentatie en de benodigde informatie voor het effectief doorlopen van een scenario in incidentmanagement en response;
- Het oefenen van de processtappen in het incident management en responseproces zodat dit sneller en effectiever doorlopen kan worden in een echte crisis.

De primaire doelstellingen kunnen bereikt worden door veel afgeleide of secundaire doelstellingen. Een selectie van 10 mogelijke secundaire doelstellingen zijn hierna (in willekeurige volgorde) opgenomen:

1. **Testen van vertaling van meldingen naar beveiligingsincidenten**: Valideren of de bestaande vertaling van meldingen en alarmeringen naar incidentcategorieën en urgenties op basis van de dreigingen, kwetsbaarheden en de te beschermen belangen effectief zijn. Effectief is hier dat ze gebruikt kunnen worden in het beschreven proces;
2. **Verbeteren van communicatie**: Valideren en oefenen van de communicatie tussen verschillende teams en afdelingen tijdens een beveiligingsincident, en het identificeren van mogelijke verbeterpunten. Denk hierbij aan de bedrijfsvoering, de IT-organisatie, speciale functies zoals een ISO, CISO en FG. Effectieve communicatie versnelt het proces en verbetert de beslissingen;
3. **Versterken van teamwerk**: Oefenen en versterken van de samenwerking en teamdynamiek binnen de beveiligingsincident en -responseteams en andere betrokken partijen tijdens de afhandeling van een incident.
4. **Identificeren van proceshiaten en zwakke punten**: Ontdekken van tekortkomingen of inefficiënties in de beschreven processen, procedures of middelen (b.v. een niet bestaande rol of een dubbelzinnige besluitvorming) die kunnen leiden tot problemen tijdens een echte situatie;
5. **Verbeteren opleiding en training**: Bieden van een veilige leeromgeving waarin deelnemers hun kennis en vaardigheden kunnen verbeteren met betrekking tot beveiligingsincident en -responsemanagement;
6. **Verhogen van bewustzijn**: Door oefening verhogen van het bewustzijn over potentiële dreigingen en risico's binnen de organisatie en hoe daarop gereageerd moet worden;
7. **Beoordelen van besluitvormingsprocessen**: Analyseren hoe besluiten worden genomen tijdens een beveiligingsincident en of deze besluiten effectief en efficiënt zijn en passend zijn binnen de mandaten voor de rollen;
8. **Ontwikkelen van actiepunten**: Genereren van concrete actiepunten en aanbevelingen voor verbeteringen die na de oefening kunnen worden geïmplementeerd als onderdeel van streven naar continue verbetering;
9. **Versterken van Relaties met Externe Partners**: Indien van toepassing, het verbeteren van de samenwerking met externe partijen zoals hulpdiensten, leveranciers of andere betrokken organisaties zodat men elkaar snel kan vinden en op voorhand weten wat men aan elkaar heeft;
10. **Evalueren van Resources en Tools**: Valideren of de beschikbare middelen, technologieën en tools adequaat zijn voor het ondersteunen van incidentresponse voor het beschreven scenario.

5 Opzet van de oefeningen

Alle scenario gebaseerde tabletop-oefeningen hebben dezelfde 3 fases. Deze worden in dit hoofstuk toegelicht. Dit is de nadere uitwerking van het raamwerk van de tabletop-oefeningen. Vervolgens worden de 3 in dit document beschreven oefeningen geïntroduceerd en wordt de relatie tusssen de drie oefeningen verder toegelicht. Na dit hoofdstuk worden de drie oefeningen verder in detail beschreven.

Hierna worden de 3 fases van iedere tabletop oefening beschreven, zoals die verder per tabletop oefening zijn uitgewerkt.

5.1 Voorbereidende fase

Doelstellingen bepalen: Stel duidelijk de doelen van de oefening vast, zoals het testen van responseplannen, het verbeteren van communicatie of het identificeren van hiaten in processen. Als hulp bij het bepalen van een specifieke set van doelstellingen die van toepassing zijn voor deze tabletop, zijn in 4.1 Doelstellingen een aantal standaard doelstellingen beschreven die door de organisatoren gebruikt kunnen worden ter inspiratie.

Deelnemers identificeren: Bepaal wie betrokken zal zijn bij de oefening, waaronder leden van het incident- & -responsemanagementteam, IT-management, CISO- en ISO-functies, de Functionaris gegevensbescherming, IT-personeel, juridische zaken, communicatie en relevante derde partijen, zoals de leveranciers van diensten en applicaties. Denk ook aan partijen zoals de CSIRT van de organisatie.

Scenario Kiezen: Ontwikkel een realistisch en relevant scenario van een beveiligingsincident dat potentiële dreigingen voor de organisatie weerspiegelt, zoals een datalek, ransomware-aanval of natuurramp. Voor de in deze beschrijving opgenomen tabletops zijn specifieke scenario’s vastgesteld maar er zijn keuzes beschikbaar voor de invulling van het scenario in de vorm van de te gebruiken data-elementen.

Agenda ontwikkelen: Maak een gestructureerde agenda die de flow van de oefening schetst, inclusief tijdsallocaties voor discussie, introductie van het scenario en debriefing.
Per tabletop is een specifieke agenda vastgesteld die uitvoerbaar moeten zijn voor het scenario. De agenda is, echter, ook afhankelijk van de mate van discussie die plaats vindt en de ruimte die hiervoor gegeven wordt. Aanpassing van de agenda in tijd zou bijvoorbeeld kunnen plaatsvinden wanneer het aantal deelnemers groot is.

Hulpbronnen verzamelen: Verzamel de nodige materialen, zoals incidentresponseplannen, relevante beleidsdocumenten, communicatietools en andere referentiedocumenten. Voor het scenario van een tabletop hebben wij aangegeven welke materialen nodig zijn. Let erop dat wanneer er aanpassingen gedaan worden aan de scenario’s ook het bestaan van de benodigde materialen geverifieerd moet worden. Ook moeten deze hulpbronnen offline beschikbaar zijn. Het toetsen van de beschikbaarheid van de hulpbronnen behoort ook bij een table top oefening. Het is belangrijk dat de security incident & response manager dit goed bij houdt en weet waar de documenten zijn bewaard.

Basisregels vaststellen: Stel richtlijnen op voor deelname, inclusief vertrouwelijkheid, respect voor verschillende meningen en een focus op leren en niet op de fouten. De basisregels zijn nodig omdat er tijdens een oefening vaak veel discussie is en mogelijk onenigheid op tafel komt, waarbij

aan tafel ook een ongelijke machtsverhouding zal zijn tussen uitvoerenden en beslissers. Belangrijk is een veilige leeromgeving te creëren.

Voorbereiding van de begelider of facilitator: Wijs een begeleider of facilitator aan die de oefening leidt, discussies beheert en ervoor zorgt dat de doelstellingen worden behaald. De persoon moet goed op de hoogte zijn van incidentbeheer en het specifieke scenario. Een begeleider of facilitator kan ook een externe zijn van een specialiseerde organisatie. In dit laatste geval zullen deze mogelijk ook een specifieke invulling geven aan de oefening. Ga in overleg met de begeleider of facilitator om te bepalen welke informatie die nodig heeft om te kunnen vaststellen of de doelstellingen gehaald zijn en waar de verbeterpunten liggen.

Technische opstelling: Zorg ervoor dat alle nodige technologie (bijv. presentatiemateriaal, videoconferentietools) aanwezig en functioneel is. Hierbij is het van belang het scenario mee te nemen in de keuze van de faciliteit. Wanneer er in de organisatie afspraken zijn voor calamiteitenlocaties is het een goed idee om hiervan gebruik te maken. De locatie kan ook voor een deel zorgdragen voor het creëren van de veilige omgeving waar er niet gestoord zal worden. Let op, de technische opstelling is alleen benodigd tijdens een table top oefening. Tijdens een daadwerkelijk incident is alleen een calamiteitenlocatie nodig.

5.2 Uitvoeren tabletop oefening

Pre-oefenbriefing: Voer een briefing uit met deelnemers om achtergrondinformatie over de oefening te geven, rollen uit te leggen en verwachtingen te verduidelijken. In de tabletop geven wij aan welke informatie vooraf gedeeld moet worden. Dit kan naar voorkeur en ervaring van de organisatie aangepast worden.

Documenteer alles: Bereid je voor om notities, discussies en beslissingen die tijdens de oefening worden gemaakt vast te leggen voor latere beoordeling en analyse. Wanneer er als doelstelling ook de communicatie en de samenwerking van de rollen worden gekozen, is het een goed plan om de sessie ook op te nemen. Hierdoor kan er een analyse van problemen en mogelijke verbeteringen plaatsvinden.

Procesdoorloop: In product "Incident Response – Procesmodel (IR-4)" zijn de processtappen voor incidentoplossing geheel uitgewerkt. Dat document beschrijft de stappen in detail om organisaties te begeleiden bij het effectief oplossen van informatiebeveiligingsincidenten. Elke processtap speelt een cruciale rol in het beheersen van een incident en het minimaliseren van de impact op de organisatie. Hieronder wordt de procestappen benoemd en met een zin uit de beschrijving van het proces toegelicht, die doorlopen moeten worden. De volledige uitleg van de stappen en de rollen die hierin acteren staat in het document "VSSR I&R IR4 – Incident & Response – Procesmodel".
Na de benoeming van de processtappen geven wij in detail aan welke activiteiten in de tabletop oefening van de deelnemers verwacht worden.

1-Preparatie

> Als onderdeel van de risicoanalyse voor beveiligingsincidenten, worden scenario's beschreven inclusief de activiteiten welke nodig zijn om de impact van het beveiligingsincident te minimaliseren.

2-Registratie en verificatie

De melding van een mogelijk beveiligingsincident wordt bij binnenkomst door de Security incident- en responsemanager vastgelegd in het incidentbeheersysteem. Dit omvat het registreren en verifiëren van belangrijke gegevens zoals de beschrijving van het mogelijke beveiligingsincident, het tijdstip van detectie (indien bekend), de bron, de initiële impact en andere relevante informatie die noodzakelijk zijn voor verdere analyse en opvolging.

3-Classificatie & Prioritering

Het beveiligingsincident wordt geanalyseerd waarbij op basis van impact en urgentie een prioriteit wordt vastgesteld.

4-Onderzoek & diagnose

In deze fase vindt nader onderzoek plaats, om de oorzaak van het beveiligingsincident te achterhalen en werkelijke impact te valideren.

5-Containment

De eerste vervolgstap in de response na definitieve vaststelling van het beveiligingsincident, is het inperken van (mogelijke) verspreiding van de oorzaak en daarmee impact van het beveiligingsincident.

6-Oplossing & herstel

Na of zelfs tijdens de voorgaande fasen Onderzoek & Diagnose en/of Containment, worden er maatregelen getroffen om het beveiligingsincident op te lossen en de IT-dienstverlening te herstellen.

7-Evaluatie

Nadat het beveiligingsincident is opgelost, wordt het geëvalueerd met analyse ter structurele verbetering van het beveiligingsincident- & responseproces in het bijzonder de responseplannen.

Hierna worden voor de hiervoor benoemde activiteiten uit het proces aangegeven welke activiteiten, wanneer moeten worden uitgevoerd in de oefening.

5.2.1 Preparatie

Wanneer: Voorafgaand aan de afhandeling van het beveiligingsincident.
Wat moet er volgens het proces gedaan worden:

- Beschikbaarheid van incidentresponseplannen: Zorg ervoor dat gedetailleerde responseplannen beschikbaar zijn in hun huidige gepubliceerde versie;
- Rollen en verantwoordelijkheden: Zorg ervoor dat alle betrokkenen duidelijk weten wat hun rol en verantwoordelijkheden zijn in geval van een beveiligingsincident;
- Hulpmiddelen en technologie: Verzamel en test alle benodigde hulpmiddelen en technologieën om te verzekeren dat ze functioneel zijn tijdens de oefening.

Wat doen we in de oefening:

- ☑ We valideren of alle informatie die we nodig hebben aanwezig is en toegankelijk;
- ☑ of alle rollen uit het proces zijn ingevuld in de oefening;
- ☑ of alle communicatiemiddelen en andere hulpmiddelen aanwezig zijn en gebruikt kunnen worden.

5.2.2 Registratie en verificatie

Wanneer: Zodra een beveiligingsprobleem wordt gemeld.
Wat moet er gedaan worden:

- Documentatie van de melding als een beveiligingsincident: Gebruik een incidentregistratiesysteem om het incident gedetailleerd te documenteren. Gedetailleerd betekent hier conform de template van het registratiesysteem;
- Verificatie van het beveiligingsincident: Verifieer de authenticiteit van de melding van het beveiligingsprobleem met de beschikbare middelen;
- Stel vast of de melding daadwerkelijk valt binnen de te hanteren definitie van een securityincident;
- Bevestiging van betrokken asset: Identificeer de getroffen asset en stel vast wat de attributen zijn, waar het asset zich bevindt en wat aan de asset gerelateerd is (IT-systemen, data en bedrijfsprocessen).

Wat doen we in de oefening:

- ☑ We doorlopen de beschreven stappen conform de procesbeschrijving met gebruik van de tooling;
- ☑ We stellen vast dat iedereen de verantwoordelijkheid voor die processtap heeft genomen en dat dit van waarde was om die processtap effectief te doorlopen.

5.2.3 Classificatie & prioritering

Wanneer: Na registratie en verificatie van de beveiligingsmelding.
Wat moet er gedaan worden:

- Classificatie: Bepaal de ernst en impact van het incident op basis van de vooraf gedefinieerde criteria uit de procesbeschrijving en/of het beleid voor beveiligingsincident management en geef het incident de juiste classificering mee;
- Prioritering: Prioriteer het incident op basis van urgentie en de potentiële bedrijfsimpact;
- Responsestrategie: Stel een strategie op voor een snelle en effectieve response gebaseerd op de vastgestelde en geverifieerde classificatie en prioritering en de aanwezigheid van hierop beschreven beveiligingsincident- en responseplannen.

Wat doen we in de oefening:

- ☑ We stellen vast of de aan het incident gerelateerde assets uit de assetregistratie te halen zijn en of die assets voldoende beschreven zijn om de impact op de bedrijfsvoering te kunnen inschatten en daarmee de classificatie van het beveiligingsincident;
- ☑ We stellen vast of de prioritering die het proces en de beleidsdocumenten geven aan dit incident voldoende is om de juiste snelheid in activiteiten en besluitvorming te realiseren;
- ☑ We stellen vast of we een specifieke of generieke beschrijving kunnen vinden om de afhandeling verder te kunnen voorzetten en indien niet aanwezig wordt die ter plekke geformeerd (zowel de strategie als de vervolgacties).

5.2.4 Onderzoek & diagnose

Wanneer: Na classificatie en prioritering.
Wat moet er gedaan worden:

- Gedetailleerd onderzoek: Voer een grondig onderzoek uit om de oorzaak van het incident te identificeren;
- Diagnose: Begrijp de omvang en impact van het incident door middel van forensisch onderzoek en analyse;
- Bewijsmateriaal verzamelen: Verzamel en documenteer bewijsmateriaal om de bevindingen te ondersteunen.

Wat doen we in de oefening:

- ☑ Deze activiteiten kunnen parallel plaatsvinden. Hoe verdelen we de aandacht?
- ☑ We doen een bepaling van de huidige omvang van het incident en de potentiële impact die het kan hebben op de betrokken assets en de bedrijfsvoering waar deze assets betrekking op hebben;
- ☑ We nemen in de bepaling van de impact het worst case scenario in ogenschouw en het meest waarschijnlijke scenario en we beperken ons niet tot onze eigen organisatie maar kijken naar de informatie en waardeketen waarin we gepositioneerd zijn;
- ☑ We bepalen of het vinden van de oorzaak en de wijze waarop dit incident heeft ontstaan nu zinvol is en prioriteit heeft, en hoe we kunnen zorgen dat er in ieder geval geen waardevolle informatie verloren gaat.

5.2.5 Containment

Wanneer: Zodra de eerste diagnose is voltooid.
Wat moet er gedaan worden:

- Maatregelen nemen: Neem onmiddellijk maatregelen om verdere schade te voorkomen en het incident in te dammen;
- Impact beperken: Beperk de impact van het incident op de bedrijfsvoering door getroffen systemen te isoleren;
- Communicatie: Informeer relevante stakeholders over de genomen stappen en de status van het incident.

Wat doen we in de oefening:

- ☑ We bepalen of de vooraf beschreven maatregelen uit de specifieke of generieke beschrijving voor securityincident response van toepassing en afdoende zijn en vullen dat aan waar we dat nodig vinden;
- ☑ We bepalen of het incident zich in een mogelijk af te schermen (netwerk) segmentatie voortdoet en of het mogelijk en zinvol is deze segmentering van de rest van onze organisatie af te schermen;
- ☑ We bepalen wie voor de isolatie verantwoordelijk is en of die gemandateerd is om dat besluit te mogen nemen;
- ☑ Indien het mandaat bij de deelnemers ontbreekt wordt contact gezocht met de gemandateerde om vast te stellen welke informatie die nodig zou moeten hebben om deze beslissing te kunnen nemen.

5.2.6 Oplossing & herstel

Wanneer: Na containment. *Let op, in sommige gevallen kan het voorkomen dat de oplossing & herstel parallel met containment wordt uitgevoerd. Maar stapsgewijs komt oplossing & herstel na containment.*
Wat moet er gedaan worden:

- Herstelwerkzaamheden: Voer de nodige herstelwerkzaamheden uit om het probleem op te lossen;
- Systemen herstellen: Breng getroffen systemen terug naar hun normale operationele status;
- Validatie: Bevestig dat alle herstelacties succesvol zijn uitgevoerd en dat het incident volledig is opgelost.

Wat doen we in de oefening:

- ☑ We stellen vast of we inzicht hebben in welke herstelacties gedaan moeten worden en wie die zou moeten uitvoeren;
- ☑ We stellen vast wie gemandateerd is voor deze herstelacties;
- ☑ We stellen vast hoe we kunnen valideren of de bedrijfsfuncties weer hersteld zijn;
- ☑ We stellen vast welke restpunten er nu nog open staan (zoals in de diagnose en eventueel het forensisch onderzoek).

5.2.7 Evaluatie (van het doorlopen incident en responseproces)

Wanneer: Na herstel.
Wat moet er gedaan worden:

- Evaluatie van de response: Evalueer de incidentresponse om te beoordelen hoe effectief de stappen waren;
- Identificatie van verbeterpunten: Identificeer hiaten en verbeterpunten in het proces;
- Documentatie van leerpunten: Documenteer de leerpunten en stel een verbeterplan op voor toekomstige incidenten.

Wat doen we in de oefening:

- ☑ We stellen vast of de informatie en documentatie die we gebruikt hebben nu voldoende waren voor de effectieve afhandeling;
- ☑ We stellen vast of de informatie over de melding, het incident en de betrokken assets voldoende en juist waren;
- ☑ We stellen vast of er geen informatie is verloren gegaan in de afhandeling;
- ☑ We stellen vast waar we te veel tijd verloren zijn in de afhandeling.

5.3 Evaluatie oefening & opvolgingsfase

Nadat de evaluatie van het doorlopen incident is afgerond wordt hier de evaluatie van de oefening beschreven.

Evaluatiecriteria: Stel criteria vast om de effectiviteit van de oefening te beoordelen, zoals responsetijden, besluitvormingsprocessen en communicatie-effectiviteit.
In principe zullen alle doelstellingen die gekozen en/of aanvullend geformuleerd worden ook beschreven moeten worden in evaluatiecriteria om vast te stellen of deze gehaald zijn.

Follow-up plan: Ontwikkel een plan voor post-oefenactiviteiten, inclusief debriefing-sessies, feedbackverzameling en actiepunten voor verbetering. Alle leerpunten van de oefening moeten gebruikt worden. Hierbij zijn de formele documenten natuurlijk van groot belang. Daarnaast zijn er minder concrete verbeterpunten die minstens even belangrijk zijn. Kennis, communicatie, begrip en empatisch vermogen zullen ook een belangrijke rol spelen tijdens een stressvol beveiligingsincident en de weerbaarheid van de organisatie beïnvloeden. Geef ook deze een plaats in de verbeterplannen.

6 Introductie van de scenario keuzes en de oefeningen

In dit hoofdstuk beschrijven we de drie oefeningen op basis van de scenario's die in de oefeningen worden behandeld. Deze beschrijving geeft voldoende informatie om tot een weloverwogen keuze van een scenario te komen. Tevens geven we aan hoe er een kans-element kan worden ingebracht in het te oefenen scenario zodat de uitvoering niet iedere keer volgens hetzelfde stramien hoeft te verlopen en een herhaling van de oefening zinvol blijft. Het kans-element wordt bereikt met een dobbelsteen en wordt hierna beschreven.

Natuurlijk staat het de organisatie vrij om ook bewuste keuzes te maken wat betreft de te hanteren incidenten of dit in een combinatie te doen.

6.1 Scenario keuze

6.1.1 Beschrijving van dobbelsteensysteem, incidenten en assets

Hier wordt het dobbelsteensysteem uitgelegd en worden de 11 incidenten als onderdeel van het scenario's en de 11 hieraan te relateren assets beschreven. Het gooien van de dobbelstenen gebeurt voor wat betreft de incidenten altijd tijdens de voorbereidende fase: Scenario kiezen. De keuze voor de assets kan zowel in de voorbereiden fase als in de start van de preparatie bij de uitvoering. Dat laatste alleen wanneer er gebruik gemakt wordt van een assetregistratiesysteem wat in de oefening ook beschikbaar is zodat de asset-informatie ter plekke beschikbaar is.

Het dobbelsteensysteem is een speelse en interactieve manier om willekeurige incidenten en getroffen assets te genereren voor de tabletop oefening. Dit systeem maakt gebruik van twee dobbelstenen, waarbij elke dobbelsteen een specifieke rol speelt in het bepalen van de uitkomst. Hier volgt een duidelijke uitleg over hoe het systeem werkt:

Werking van het dobbelsteensysteem:

Gebruik van Twee Dobbelstenen (1-6):

- De begeleider of facilitator gooit altijd met twee dobbelstenen of met twee keer een enkele dobbelsteen. Dit zorgt voor een breder scala aan mogelijke uitkomsten en verhoogt de variatie in de scenario's.

Toewijzing van Incidenten en Assets:

- Voor de oefening worden de incidenten en assets genummerd. Dit betekent dat elke incident en asset een uniek nummer krijgt dat overeenkomt met de mogelijke uitkomsten van de dobbelstenen;
- Bijvoorbeeld, als er 11 incidenten zijn, kunnen ze worden genummerd van 2 tot 12. Voor de assets geldt hetzelfde. Bij het gooien van twee dobbelstenen kan je nooit eindigen op 1, daarom beginnen we bij de incidenten en assets op 2.

Kanttekening voor het gebruik van twee dobbelstenen is dat de uitkomst 7 vaker zal voorkomen dan andere uitkomsten. Dit is te voorkomen door gebruik te maken van online oplossingen die een virtuele 'dobbelsteen' van 12 kanten simuleert. Dit kan bijvoorbeeld op de website Random.org, let erop dat incidenten en assets in deze situatie wel vanaf 1 genummerd kunnen worden.

Voorbeeld van een dobbelsteenspel:

Incidenten: Genummerd van 2 tot 12.

Assets: Genummerd van 2 tot 12.

Stap 1: Begeleider of facilitator gooit met twee dobbelstenen en krijgt een som van 7.
Stap 2: Het 7e incident wordt gekozen (bijvoorbeeld "Denial of Service (DoS) aanval").
Stap 3: Begeleider of facilitator gooit opnieuw met de dobbelstenen en krijgt een som van 6.
Stap 4: Het 6e asset wordt gekozen (bijvoorbeeld "Cloud servers").
Stap 5: Het gekozen scenario voor de oefening is een DoS-aanval op de cloud servers.

Dit dobbelsteensysteem zorgt voor een dynamische en flexibele oefening die begeleider of facilitator helpt om verschillende scenario's te verkennen en hun vaardigheden in incidentbeheer te verbeteren. Het gooien van de dobbelstenen geeft ook een speels element wat ervoor zorgt dat deze serieuze oefening toch leuk is om te doen.

Incidenten om te kiezen:

2. Datalek: Ongeoorloofde blootstelling van gevoelige informatie.
3. Ransomware-aanval: Kwaadaardige software die gegevens versleutelt en losgeld eist.
4. Phishing aanval: Fraude via e-mail om gevoelige informatie te verkrijgen.
5. Insider threat: Bedreiging van binnen de organisatie door medewerkers.
6. Malware infectie: Schadelijke software die systemen infecteert.
7. Denial of Service (DoS) aanval: Overbelasting van netwerk of systemen om dienstverlening te verstoren.
8. Verlies van apparatuur: Verlies van fysieke apparaten met gevoelige informatie.
9. Ongeautoriseerde toegang: Toegang tot systemen door onbevoegden.
10. Verkeerd geconfigureerde systemen: Onjuiste systeeminstellingen die beveiligingsrisico's veroorzaken.
11. Fysieke beveiligingsinbreuk: Ongeautoriseerde fysieke toegang tot faciliteiten.
12. Technische storing: Een onverwachte uitval of storing van kritieke systemen of infrastructuur, zoals serverstoringen, netwerkuitval of storingen in datacenters, die de bedrijfsvoering beïnvloeden.

Assets om te kiezen:

2. Databases: Opslagplaatsen voor gestructureerde gegevens.
3. Netwerkapparatuur: Apparaten die netwerkverbindingen mogelijk maken.
4. Laptops: Draagbare computers gebruikt door medewerkers.
5. Mobiele apparaten: Smartphones en tablets gebruikt voor zakelijke doeleinden.
6. Cloud servers: Externe servers voor dataopslag en applicatiehosting.
7. Back-ups: Kopieën van gegevens voor hersteldoeleinden.
8. E-mail systemen: Platformen voor zakelijke communicatie.
9. Webapplicaties: Online softwareapplicaties die diensten leveren.
10. Personeelsgegevens: Gevoelige informatie over werknemers.
11. Klantgegevens: Gevoelige informatie over klanten.
12. Productiesystemen: Systemen die essentiële bedrijfsprocessen ondersteunen.

6.2 Introductie van de drie scenario's

In dit hoofdstuk worden de drie tabletop-scenario's geïntroduceerd, die elk een andere procesfase van beveiligingsincident- en responsemanagement binnen de organisatie vertegenwoordigen. Deze oefeningen lopen op in complexiteit: van een beginnende Informatiebeveiligingsmelding, via een volwaardig incident tot aan een crisis. Door de oefeningen in deze volgorde te doorlopen, kan de organisatie stapsgewijs inzicht krijgen in de sterke punten en verbeterkansen van haar response- en escalatieprocedures. Ook kan het vaste team van leiders, facilitators en begeleiders op elkaar ingespeeld worden. In de eerste oefening zal veel aandacht zijn voor de beschikbaarheid en juistheid van de documentatie. De andere oefeningen kan meer aandacht besteed worden aan de integratie en de response.

6.2.1 Tabletop I: Informatiebeveiligingsmelding uitloop

In deze oefening ligt de nadruk op het vroegtijdig herkennen en beoordelen van een potentiële dreiging. Zodra een eerste melding binnenkomt, wordt getest hoe snel en effectief de organisatie reageert, welke teams worden ingeschakeld en hoe de communicatie verloopt. Het hoofddoel is inzicht krijgen in de procedure voor melding en eerste escalatie, zodat mogelijke risico's snel worden geïdentificeerd en onder controle gebracht.

6.2.2 Tabletop II: Beveiligingsincident uitloop

Deze sessie gaat een stap verder: het beveiligingsincident is inmiddels bevestigd en de impact neemt toe. De organisatie moet haar incidentresponse- en escalatieprocedures op hoger niveau coördineren. De focus ligt op het werken met multidisciplinaire teams (bijv. IT, management, legal, communicatie) om het incident in te dammen op basis van een vooraf vastgesteld responseplan, verdere schade te beperken en helder te communiceren naar interne en externe stakeholders.

6.2.3 Tabletop III: Crisis escalatie oefening

In de derde oefening is de situatie geëscaleerd tot een crisis. De complexiteit is hoog en kan verstrekkende gevolgen hebben voor de bedrijfscontinuïteit, reputatie en financiële stabiliteit. De organisatie test hier haar escalatieproces om te komen tot een crisisstructuur, strategische besluitvorming onder druk en de mate van samenwerking tussen alle betrokken afdelingen. De nadruk ligt op snelle besluitvorming, kennis van de crisisteams en het mandaat om een crisis op te starten met heldere communicatie naar alle betrokken partijen.

6.3 Samenhang van de oefeningen

De oefeningen zijn opgebouwd rondom verschillende fasen van een incidentafhandeling, van de eerste informatiebeveiligingsmelding tot de uitloop van een daadwerkelijk incident en uiteindelijk de escalatie naar een crisis. De drie tabletop-oefeningen vormen samen een logische opbouw in de response op dreigingen. Deze stapsgewijze aanpak geeft teams de kans om in elke fase van de incidentresponse de procedures en communicatie bij beveiligingsincidenten te toetsen, te verfijnen en op elkaar af te stemmen. Zo groeit de organisatie van basisresponse naar het effectief beheersen van de escalatie naar een crisis, waarbij de inzichten uit eerdere oefeningen direct van pas komen in de volgende fase.

Een ander voordeel van deze wijze van indeling is dat er makkelijker gekozen kan worden om de eerste of tweede oefening te verlengen wanneer de tijd dat toestaat en de volgend elementen te kiezen uit de volgende oefening.

6.4 Handvatten voor het gebruik van het raamwerk

Dit hoofdstuk biedt praktische tips en richtlijnen voor het gebruik van het raamwerk tijdens de tabletop oefening. Het helpt organisatoren om de oefening effectief te plannen en uit te voeren.

Handvatten:

- Selecteer de doelstellingen die het beste passen bij de behoeften van uw organisatie en probeer niet alle doelstellingen te selecteren;
- Bepaal de deelnemers zorgvuldig om ervoor te zorgen dat alle relevante partijen vertegenwoordigd zijn. Het is belangrijk dat de meest ervaren resources in een eerste oefening meedoen. Er is inleving nodig en aannames moeten gemaakt worden die kennis en ervaring vereisen. In een herhaling van de oefening kan dat losgelaten worden;
- Kies het scenario en gebruik de dobbelstenen om willekeurige incidenten en assets te genereren. Doe dit voorafgaand aan de werkelijke oefening zodat er door de facilitator extra informatie over de organisatie de assets beschikbaar kan worden gesteld;
- Ontwikkel een agenda die de tijd efficiënt benut en ruimte biedt voor discussie. Besteed de rol van time-manager uit aan een van de deelnemers zodat de focus van de oefenleider op de inhoud kan zijn;
- Verzamel alle benodigde hulpbronnen en zorg ervoor dat ze beschikbaar zijn tijdens de oefening. Dit omvat het identificeren en organiseren van materialen zoals scenario's, checklists, relevante documentatie en technische middelen zoals projectoren en videoconferentie-apparatuur;
- Stel basisregels op om een veilige en respectvolle leeromgeving te creëren. Door deze basisregels aan het begin van de oefening te communiceren, zorgt de begeleider ervoor dat iedereen zich bewust is van de gedragsverwachtingen en dat de oefening in een harmonieuze sfeer plaatsvindt;
- Bereid de facilitator voor op het leiden van de oefening en het beheren van discussies. Dit kan worden bereikt door een voorbereidende bijeenkomst te houden waarin de facilitator wordt gebrieft over zijn of haar rol en verantwoordelijkheden. De facilitator moet ook worden getraind in technieken voor het leiden van discussies, het stellen van gerichte vragen en het beheren van de dynamiek tussen deelnemers;
- Zorg voor de technische opstelling zodat alle technologieën klaar voor gebruik zijn. Het is ook belangrijk om een technische ondersteuningsteam of contactpersoon beschikbaar te hebben om eventuele technische problemen snel op te lossen. Dit minimaliseert onderbrekingen en zorgt ervoor dat de focus op de inhoud van de oefening blijft;
- Voer een pre-oefenbriefing uit om deelnemers voor te bereiden en verwachtingen te managen. Tijdens deze briefing kunnen deelnemers vragen stellen en eventuele onduidelijkheden verduidelijken. Dit helpt om iedereen op dezelfde lijn te krijgen en zorgt ervoor dat deelnemers zich comfortabel en voorbereid voelen om actief deel te nemen aan de oefening;
- Stel evaluatiecriteria vast om de effectiviteit van de oefening te beoordelen. Dit is essentieel om de effectiviteit van de tabletop oefening te meten. Deze criteria kunnen betrekking hebben op verschillende aspecten, zoals de snelheid en nauwkeurigheid van de response, de kwaliteit van de communicatie en samenwerking, en de mate waarin de doelstellingen van de oefening zijn bereikt. Door deze criteria vooraf te communiceren, weten deelnemers waarop ze worden beoordeeld en kunnen begeleiders en facilitators gerichte feedback geven;
- Documenteer alles voor latere beoordeling en verbetering. Doe dit door naast een oefenleider ook iemand aan te stellen die verantwoordelijk is voor de vastlegging. Het is aan te raden om iemand aan te stellen die specifiek verantwoordelijk is voor de

vastlegging van alle belangrijke discussies, beslissingen en acties die tijdens de oefening worden genomen. Dit zorgt ervoor dat niets over het hoofd wordt gezien en dat er een gedetailleerd verslag is voor latere analyse en follow-up.

Ontwikkel een follow-up plan om de leerpunten te implementeren en de organisatie te versterken. Een follow-up plan is essentieel om de leerpunten uit de tabletop oefening te implementeren en de organisatie te versterken. Dit plan moet concrete actiepunten bevatten, met toegewezen verantwoordelijkheden en deadlines, om ervoor te zorgen dat verbeteringen worden doorgevoerd. Het is ook belangrijk om regelmatige evaluaties en voortgangsrapportages in te plannen om de implementatie van de leerpunten te monitoren en de effectiviteit van de verbeteringen te beoordelen.

7 Tabletop I - Informatiebeveiligingsmelding uitloop

Deze tabletop oefening richt zich op het proces van het ontvangen en verwerken van informatiebeveiligingsmeldingen.

Voor het uitvoeren van de tabletop oefening volgen we het raamwerk beschreven in hoofdstuk 5 “Opzet van de oefeningen”.

7.1 Voorbereidende fase

Tijdens de voorbereidende fase waarborgt de facilitator dat alle hulpbronnen beschikbaar zijn en dat alle zaken op de juiste wijze zijn geregeld.

7.1.1 Doelstellingen bepalen

Zie hoofdstuk 4.1 Doelstellingen voor het bepalen van de doelstelling voor de tabletop informatiebeveiligingsmelding opvolging

7.1.2 Deelnemers identificeren

De volgende deelnemers zijn benodigd bij een informatiebeveiligingsmelding:

- IT-Security-incident en responsemanager (SIRM);
- IT-personeel en systeem- en netwerkbeheerders;
- Communicatieteam;
- Belanghebbenden en derde partijen.

7.1.3 Scenario Kiezen

Voor het kiezen van een scenario maken we gebruik van het dobbelsteensysteem beschreven in hoofdstuk 6.1 Beschrijving van dobbelsteensysteem, incidenten en assets.

7.1.4 Agenda ontwikkelen

Totale tijdsduur van scenario: 4 uur

In deze tijdsduur is er 1 uur en een kwartier voorzien voor de activiteiten met pauze die de oefening vorm geven (nr. 1, 2, 4 en 8) en 3 uren voor het doorlopen van het scenario (nr. 3, 5 ,6 en 7). Voor deze 3 uren is een verwijzing naar de procesdoorloop activiteiten meegeven naast de tijdsindicatie).

Agenda:

1. Introductie, agenda, hulpbronnen uitgeven en basisregels bespreken (15 minuten)
2. Pre-oefenbriefing (15 minuten)
3. Uitvoeren processtap preparatie (45 minuten)
4. Pauze (15 minuten)
5. Uitvoeren processtap registratie & verificatie (45 minuten)
6. Uitvoeren processtap classificatie en prioritering (45 minuten)
7. Uitvoeren processtap evaluatie incident (30 minuten)
8. Evaluatie oefening en opvolgingsfase (30 minuten)

7.1.5 Hulpbronnen verzamelen

- ☐ (Beveiligings)Incidentmanagement & response proces documentatie ;
- ☐ Incidentmanagement procedures en -werkinstructies;
- ☐ Incidentresponseplannen (generiek en/of specifieke plannen);
- ☐ Communicatiebeleid en procedures;
- ☐ Contactinformatie van alle betrokkenen op basis van de gekozen assets;
- ☐ Documentatie over classificatie- en prioriteringscriteria.

7.1.6 Basisregels vaststellen

- ☐ Vertrouwelijkheid van de informatie waarborgen;
- ☐ Respect voor alle deelnemers en hun bijdragen;
- ☐ Focus op leren en verbeteren, niet op schuld toewijzen;
- ☐ Actieve deelname en constructieve feedback.

7.1.7 Voorbereiding van de begeleider of facilitator

- ☐ De begeleider of facilitator en opdrachtgever bepalen de doelstelling en het scenario. In het scenario kan wanneer gewenst een kas-element ingebracht worden d.m.v. het gooien van de dobbelstenen;
- ☐ De facilitator zorgt ervoor dat alle hulpbronnen beschikbaar en aanwezig zijn;
- ☐ Zorg voor een veilige en rustige werkomgeving;
- ☐ Zorg ervoor dat alle deelnemers zijn geïdentificeerd en de oefening hebben geaccepteerd;
- ☐ Een interne senior IT-manager met ervaring in incidentbeheer;

- ☐ Voorgaande leerervaringen ophalen en hierop reflecteren;
- ☐ Follow-up meeting leiden en actiepunten concreet maken.

7.1.8 Technische opstelling

- ☐ Voorzien van presentatiemateriaal;
- ☐ Instellen van videoconferentietools voor deelnemers op afstand (indien het niet fysiek kan);
- ☐ Toegang tot relevante systemen en logs (indien nodig);
- ☐ Een rustige en ongestoorde ruimte voor de oefening.

7.2 Uitvoering tabletop oefening

Tijdens de tabletop-oefening worden de vooraf opgestelde scenario's uitgevoerd. Deze interactieve sessie biedt deelnemers de mogelijkheid om samen te werken, strategische beslissingen te nemen en potentiële reacties op incidenten te verkennen in een gesimuleerde omgeving.

7.2.1 Pre-oefenbriefing

- ☐ Uitleg van het doel, scenario, rollen en verantwoordelijkheden;
- ☐ Overzicht van de agenda;
- ☐ Verwachting omtrent actieve deelname en vertrouwelijkheid.

7.2.2 Documenteer alles

- ☐ Gedetailleerde notities van alle onbeantwoorde vragen;
- ☐ Gedetailleerde notities van issues, acties en beslissingen die niet zijn ingevuld;
- ☐ Opname van de sessie voor latere analyse;
- ☐ Beslissingen en actiepunten vastleggen voor follow-up.

7.2.3 Processtappen voor incidentoplossing

Tijdens de informatiebeveiligingsmelding opvolging gaan we nog niet van een incident uit, wel zijn de stappen voor de eerste fase hetzelfde als bij een incident.

7.2.3.1 1-Preparatie (als onderdeel van het incident en responseproces)

Wanneer: Voorafgaand aan de afhandeling van het beveiligingsincident.
Wat moet er volgens het proces gedaan worden:

- ➢ Beschikbaarheid van incidentresponseplannen: Zorg ervoor dat gedetailleerde responseplannen beschikbaar zijn in hun huidige gepubliceerde versie;
- ➢ Rollen en verantwoordelijkheden: Zorg ervoor dat alle betrokkenen duidelijk weten wat hun rol en verantwoordelijkheden zijn in geval van een beveiligingsincident;
- ➢ Hulpmiddelen en technologie: Verzamel en test alle benodigde hulpmiddelen en technologieën om te verzekeren dat ze functioneel zijn tijdens de oefening;

Wat doen we in de oefening:

- ☑ We valideren of alle informatie die we nodig hebben aanwezig is en toegankelijk;
- ☑ of alle rollen uit het proces zijn ingevuld in de oefening;
- ☑ of alle communicatiemiddelen en andere hulpmiddelen aanwezig zijn en gebruikt kunnen worden.

7.2.3.2 2-Registratie en verificatie

Wanneer: Zodra een beveiligingsprobleem wordt gemeld.
Wat moet er gedaan worden:

- ➢ Documentatie van de melding als een beveiligingsincident: Gebruik een incidentregistratiesysteem om het incident gedetailleerd te documenteren. Gedetailleerd betekent hier conform de template van het registratiesysteem;
- ➢ Verificatie van het beveiligingsincident: Verifieer de authenticiteit van de melding van het beveiligingsprobleem met de beschikbare middelen;
- ➢ Stel vast of de melding daadwerkelijk valt binnen de te hanteren definitie van een securityincident;
- ➢ Bevestiging van betrokken asset: Identificeer de getroffen asset en stel vast wat de attributen zijn, waar het asset zich bevindt en wat aan de asset gerelateerd is (IT-systemen, data en bedrijfsprocessen).

Wat doen we in de oefening:

- ☑ We doorlopen de beschreven stappen conform de procesbeschrijving met gebruik van de tooling;
- ☑ We stellen vast dat iedereen de verantwoordelijkheid voor die processtap heeft genomen en dat dit van waarde was om die processtap effectief te doorlopen.

7.2.3.3 3-Classificatie & prioritering

Wanneer: Na registratie en verificatie van de beveiligingsmelding.
Wat moet er gedaan worden:

- ➢ Classificatie: Bepaal de ernst en impact van het incident op basis van de vooraf gedefinieerde criteria uit de procesbeschrijving en/of het beleid voor beveiligingsincident management en geef het incident de juiste classificering mee;
- ➢ Prioritering: Prioriteer het incident op basis van urgentie en de potentiële bedrijfsimpact;
- ➢ Responsestrategie: Stel een strategie op voor een snelle en effectieve response gebaseerd op de vastgestelde en geverifieerde classificatie en prioritering en de aanwezigheid van hierop beschreven beveiligingsincident- en responseplannen.

Wat doen we in de oefening:

- ☑ We stellen vast of de aan het incident gerelateerde assets uit de assetregistratie te halen zijn en of die assets voldoende beschreven zijn om de impact op de bedrijfsvoering te kunnen inschatten en daarmee de classificatie van het beveiligingsincident;
- ☑ We stellen vast of de prioritering die het proces en de beleidsdocumenten geven aan dit incident voldoende is om de juiste snelheid in activiteiten en besluitvorming te realiseren;

- ☑ We stellen vast of we een specifieke of generieke beschrijving kunnen vinden om de afhandeling verder te kunnen voorzetten en indien niet aanwezig wordt die ter plekke geformeerd (zowel de strategie als de vervolgacties).

7.2.3.4 Evaluatie (van het doorlopen incident en responseproces)

Wanneer: Na herstel.
Wat moet er gedaan worden:

- ➢ Evaluatie van de response: Evalueer de incidentresponse om te beoordelen hoe effectief de stappen waren;
- ➢ Identificatie van verbeterpunten: Identificeer hiaten en verbeterpunten in het proces;
- ➢ Documentatie van leerpunten: Documenteer de leerpunten en stel een verbeterplan op voor toekomstige incidenten.

Wat doen we in de oefening:

- ☑ We stellen vast of de informatie en documentatie die we gebruikt hebben nu voldoende waren voor de effectieve afhandeling;
- ☑ We stellen vast of de informatie over de melding, het incident en de betrokken assets voldoende en juist waren;
- ☑ We stellen vast of er geen informatie is verloren gegaan in de afhandeling;
- ☑ We stellen vast waar we te veel tijd verloren zijn in de afhandeling.

7.3 Evaluatie oefening & opvolgingsfase

In deze fase bespreekt de facilitator zijn bevindingen uit de tabletop-oefening. De evaluatie richt zich op het identificeren van sterke punten en verbeterpunten, en resulteert in specifieke actiepunten die het team moet opvolgen om de effectiviteit te vergroten.

7.3.1 Evaluatiecriteria

- ☐ Beoordeel de effectiviteit van de melding en de initiële response;
- ☐ Snelheid en duidelijkheid van communicatie:
- ☐ Besluitvormingsprocessen en hun kwaliteit;
- ☐ Evalueer de classificatie- en prioriteringsprocessen.

7.3.2 Follow-up plan

- ☐ Opstellen van actiepunten voor verbeterpunten;
- ☐ Debriefing sessie met alle deelnemers;
- ☐ Implementatie van leerpunten in het incidentresponseplan en procedures.

7.4 Resultaat tabletop oefening

De tabletop oefening heeft de volgende kernresultaten opgeleverd:

- Verbeterde classificatie: De oefening heeft duidelijkheid verschaft over de huidige classificatiecriteria voor incidenten. Aanbevelingen zijn gedaan om deze criteria te verfijnen en te standaardiseren, zodat incidenten nauwkeuriger en consistenter kunnen worden geclassificeerd, wat leidt tot een effectievere incidentresponse;
- Verhoogde samenwerking: De oefening heeft geleid tot betere communicatie tussen verschillende teams, wat essentieel is voor een gecoördineerde incidentresponse. Nieuwe protocollen zijn ontwikkeld om de samenwerking en informatie-uitwisseling te verbeteren, waardoor teams sneller en efficiënter kunnen reageren op incidenten;
- Identificatie van verbeterpunten: Tijdens de oefening zijn hiaten en inefficiënties in het huidige incident- & responsemanagementproces blootgelegd. Deze zijn vertaald naar duidelijke actiepunten met verantwoordelijkheden, wat zorgt voor een gerichte aanpak om de zwakke punten aan te pakken en de paraatheid te verbeteren;
- Verhoogd bewustzijn: De deelnemers hebben een groter inzicht verkregen in de verschillende informatiebeveiligingsrisico's waarmee de organisatie te maken kan krijgen. Op basis van deze inzichten zijn aanbevelingen gedaan voor gerichte training en bewustwordingscampagnes om de kennis van medewerkers te vergroten;
- Documentatie: Alle discussies, beslissingen en leerervaringen zijn gedetailleerd vastgelegd in een eindrapport. Deze documentatie dient als een waardevol naslagwerk voor toekomstige oefeningen en helpt bij de voortdurende verbetering van het incident- & responsemanagementproces en bijhorende procedures;
- Evaluatie van plannen: De bestaande incidentresponseplannen zijn grondig beoordeeld tijdens de oefening. Op basis van de bevindingen zijn voorstellen voor aanpassingen en verbeteringen gedaan om deze plannen beter af te stemmen op de actuele dreigingen en organisatorische behoeften, wat bijdraagt aan een robuustere incidentresponse.

8 Tabletop II - Beveiligingsincident uitloop

Deze tabletop oefening richt zich op het proces van het ontvangen en verwerken van een beveiligingsincident.

Voor het uitvoeren van de tabletop oefening volgen we het raamwerk beschreven in hoofdstuk 5 "Opzet van de oefeningen".

8.1 Voorbereidende fase

Tijdens de voorbereidende fase waarborgt de facilitator dat alle hulpbronnen beschikbaar zijn en dat alle zaken op de juiste wijze zijn geregeld.

8.1.1 Doelstellingen bepalen

Zie hoofdstuk 4.14.1 Doelstellingen voor het bepalen van de doelstelling voor de tabletop incident uitloop.

8.1.2 Deelnemers identificeren

De volgende deelnemers zijn benodigd bij een incident.

- ☐ ISRM
- ☐ Security analist
- ☐ Security incident responder
- ☐ Juridische en compliance officers.
- ☐ IT-personeel en applicatie, systeem- en netwerkbeheerders
- ☐ Communicatieteam
- ☐ Belanghebbenden en derde partijen

8.1.3 Scenario kiezen

Voor het kiezen van een scenario maken we gebruik van het dobbelsteensysteem beschreven in hoofdstuk 6.1.1 Beschrijving van dobbelsteensysteem, incidenten en assets.

8.1.4 Agenda ontwikkelen

Totale tijdsduur van scenario: 5 uur

In deze tijdsduur is er 1 uur en een kwartier voorzien voor de activiteiten met pauzes die de oefening vorm geven (nr. 1, 2, 4, 7 en 11) en 4 uren voor het doorlopen van het scenario (nr. 3, 4, 5 ,6, 8, 9 en 10). Voor deze 4 uren is een verwijzing naar de procesdoorloop activiteiten meegeven naast de tijdsindicatie).

Agenda:

1. Introductie, agenda, hulpbronnen uitgeven en basisregels bespreken (15 minuten)
2. Pre-oefenbriefing (15 minuten)
3. Uitvoeren processtap preparatie (20 minuten)
4. Uitvoeren processtap registratie & verificatie (30 minuten)

5. Uitvoeren processtap classificatie & prioritering (30 minuten)
6. Uitvoeren processtap onderzoek & diagnose (30 minuten)
7. Pauze (15 minuten)
8. Uitvoeren processtap containment (45 minuten)
9. Uitvoeren processtap oplossing & herstel (45 minuten
10. Uitvoeren processtap evaluatie incident (30 minuten)
11. Evaluatie oefening en opvolging (30 minuten)

8.1.5 Hulpbronnen verzamelen

- ☐ (Beveiligings)Incidentmanagement & response procesdocumentatie;
- ☐ Incidentmanagement procedures en -werkinstructies;
- ☐ Incidentresponseplannen (generiek en/of specifieke plannen);
- ☐ Communicatiebeleid en procedures;
- ☐ Contactinformatie van alle betrokkenen op basis van de gekozen assets;
- ☐ Documentatie over incidentoplossingen (Zie "Incident Response – Procesmodel (IR-4)");
- ☐ Toegang tot systeemlogs en monitoringtools.

8.1.6 Basisregels vaststellen

- ☐ Vertrouwelijkheid van de informatie waarborgen;
- ☐ Respect voor alle deelnemers en hun bijdragen;
- ☐ Focus op leren en verbeteren, niet op schuld toewijzen;
- ☐ Actieve deelname en constructieve feedback.

8.1.7 Voorbereiding van de begeleider of facilitator

- ☐ De begeleider of facilitator en opdrachtgever bepalen de doelstelling en het te selecteren scenario d.m.v. het gooien van de dobbelstenen;
- ☐ De facilitator zorgt ervoor dat alle hulpbronnen beschikbaar en aanwezig zijn;
- ☐ Zorg voor een veilige en rustige werkomgeving;
- ☐ Zorg ervoor dat alle deelnemers zijn geïdentificeerd en de oefening hebben geaccepteerd;
- ☐ Een interne senior IT-manager met ervaring in beveiligingsincidentmanagement;
- ☐ Een ervaren IT-manager met kennis van technische storingen;
- ☐ Voorgaande leerervaringen ophalen en hierop reflecteren;
- ☐ Follow-up meeting leiden en actiepunten concreet maken.

8.1.8 Technische opstelling

- ☐ Voorzien van presentatiemateriaal;
- ☐ Instellen van videoconferentietools voor deelnemers op afstand (indien het niet fysiek kan);
- ☐ Toegang tot relevante systemen en logs;
- ☐ Een rustige en ongestoorde ruimte voor de oefening.

8.2 Uitvoeren tabletop oefening

Tijdens de tabletop-oefening worden de vooraf opgestelde scenario's uitgevoerd. Deze interactieve sessie biedt deelnemers de mogelijkheid om samen te werken, strategische beslissingen te nemen en potentiële reacties op incidenten te verkennen in een gesimuleerde omgeving.

8.2.1 Pre-oefenbriefing

- ☐ Uitleg van het doel, scenario, rollen en verantwoordelijkheden;
- ☐ Overzicht van de agenda;
- ☐ Verwachting omtrent actieve deelname en vertrouwelijkheid;
- ☐ Technische voorbereiding;
- ☐ Communicatielijnen oefenen.

8.2.2 Documenteer alles

- ☐ Gedetailleerde notities van alle onbeantwoorde vragen;
- ☐ Gedetailleerde notities van issues, acties en beslissingen die niet zijn ingevuld;
- ☐ Opname van de sessie voor latere analyse;
- ☐ Beslissingen en actiepunten vastleggen voor follow-up.

8.2.3 Processtappen voor incidentoplossing

Tijdens de beveiligingsincident uitloop gaan we uit van een incident, waarbij alle stappen binnen het proces moeten worden uitgevoerd.

8.2.3.1 1-Preparatie

Wanneer: Voorafgaand aan de afhandeling van het beveiligingsincident.
Wat moet er volgens het proces gedaan worden:

- ➢ Beschikbaarheid van beveiligingsincidentresponseplannen: Zorg ervoor dat gedetailleerde responseplannen beschikbaar zijn en regelmatig worden bijgewerkt;
- ➢ Rollen en verantwoordelijkheden: Zorg ervoor dat alle betrokkenen duidelijk weten wat hun rol en verantwoordelijkheden zijn in geval van een beveiligingsincident;
- ➢ Hulpmiddelen en technologie: Verzamel en test alle benodigde hulpmiddelen en technologieën om te verzekeren dat ze functioneel zijn tijdens een beveiligingsincident.

Wat doen we in de oefening:

- ☑ We valideren of alle informatie die we nodig hebben aanwezig is en toegankelijk;
- ☑ of alle rollen uit het proces zijn ingevuld in de oefening;
- ☑ of alle communicatiemiddelen en andere hulpmiddelen aanwezig zijn en gebruikt kunnen worden.

8.2.3.2 2-Registratie en verificatie

Wanneer: Zodra een beveiligingsprobleem wordt gemeld.
Wat moet er gedaan worden:

- ➢ Documentatie van de melding als een beveiligingsincident: Gebruik een incidentregistratiesysteem om het incident gedetailleerd te documenteren. Gedetailleerd betekent hier conform de template van het registratiesysteem;
- ➢ Verificatie van het beveiligingsincident: Verifieer de authenticiteit van de melding van het beveiligingsprobleem met de beschikbare middelen;
- ➢ Stel vast of de melding daadwerkelijk valt binnen de te hanteren definitie van een securityincident;
- ➢ Bevestiging van betrokken asset: Identificeer de getroffen asset en stel vast wat de attributen zijn, waar het asset zich bevindt en wat aan de asset gerelateerd is (IT-systemen, data en bedrijfsprocessen).

Wat doen we in de oefening:

- ☑ We doorlopen de beschreven stappen conform de procesbeschrijving met gebruik van de tooling;
- ☑ We stellen vast dat iedereen de verantwoordelijkheid voor die processtap heeft genomen en dat dit van waarde was om die processtap effectief te doorlopen.

8.2.3.3 3-Classificatie & prioritering

Wanneer: Na registratie en verificatie van de beveiligingsmelding.
Wat moet er gedaan worden:

- ➢ Classificatie: Bepaal de ernst en impact van het incident op basis van de vooraf gedefinieerde criteria uit de procesbeschrijving en/of het beleid voor beveiligingsincident management en geef het incident de juiste classificering mee;
- ➢ Prioritering: Prioriteer het incident op basis van urgentie en de potentiële bedrijfsimpact;
- ➢ Responsestrategie: Stel een strategie op voor een snelle en effectieve response gebaseerd op de vastgestelde en geverifieerde classificatie en prioritering en de aanwezigheid van hierop beschreven beveiligingsincident- en responseplannen.

Wat doen we in de oefening:

- ☑ We stellen vast of de aan het incident gerelateerde assets uit de assetregistratie te halen zijn en of die assets voldoende beschreven zijn om de impact op de bedrijfsvoering te kunnen inschatten en daarmee de classificatie van het beveiligingsincident;
- ☑ We stellen vast of de prioritering die het proces en de beleidsdocumenten geven aan dit incident voldoende is om de juiste snelheid in activiteiten en besluitvorming te realiseren;

- ☑ We stellen vast of we een specifieke of generieke beschrijving kunnen vinden om de afhandeling verder te kunnen voorzetten en indien niet aanwezig wordt die ter plekke geformeerd (zowel de strategie als de vervolgacties).

8.2.3.4 4-Onderzoek & diagnose

Wanneer: Na classificatie en prioritering.
Wat moet er gedaan worden:

- ➢ Gedetailleerd onderzoek: Voer een grondig onderzoek uit om de oorzaak van het incident te identificeren;
- ➢ Diagnose: Begrijp de omvang en impact van het incident door middel van forensisch onderzoek en analyse;
- ➢ Bewijsmateriaal verzamelen: Verzamel en documenteer bewijsmateriaal om de bevindingen te ondersteunen.

Wat doen we in de oefening:

- ☑ Deze activiteiten kunnen parallel plaatsvinden. Hoe verdelen we de aandacht?
- ☑ We doen een bepaling van de huidige omvang van het incident en de potentiële impact die het kan hebben op de betrokken assets en de bedrijfsvoering waar deze assets betrekking op hebben;
- ☑ We nemen in de bepaling van de impact het worst case scenario in ogenschouw en het meest waarschijnlijke scenario en we beperken ons niet tot onze eigen organisatie maar kijken naar de informatie en waardeketen waarin we gepositioneerd zijn;
- ☑ We bepalen of het vinden van de oorzaak en de wijze waarop dit incident heeft ontstaan nu zinvol is en prioriteit heeft, en hoe we kunnen zorgen dat er in ieder geval geen waardevolle informatie verloren gaat.

8.2.3.5 5-Containment

Wanneer: Zodra de eerste diagnose is voltooid.
Wat moet er gedaan worden:

- ➢ Maatregelen nemen: Neem onmiddellijk maatregelen om verdere schade te voorkomen en het incident in te dammen;
- ➢ Impact beperken: Beperk de impact van het incident op de bedrijfsvoering door getroffen systemen te isoleren;
- ➢ Communicatie: Informeer relevante stakeholders over de genomen stappen en de status van het incident.

Wat doen we in de oefening:

- ☑ We bepalen of de vooraf beschreven maatregelen uit de specifieke of generieke beschrijving voor securityincident response van toepassing en afdoende zijn en vullen dat aan waar we dat nodig vinden;
- ☑ We bepalen of het incident zich in een mogelijk af te schermen (netwerk) segmentatie voortdoet en of het mogelijk en zinvol is deze segmentering van de rest van onze organisatie af te schermen;
- ☑ We bepalen wie voor de isolatie verantwoordelijk is en of die gemandateerd is om dat besluit te mogen nemen;

- ☑ Indien het mandaat bij de deelnemers ontbreekt wordt contact gezocht met de gemandateerde om vast te stellen welke informatie die nodig zou moeten hebben om deze beslissing te kunnen nemen.

8.2.3.6 6-Oplossing & herstel

Wanneer: Na containment. *Let op, in sommige gevallen kan het voorkomen dat de oplossing & herstel parallel met containment wordt uitgevoerd. Maar stapsgewijs komt oplossing & herstel na containment.*
Wat moet er gedaan worden:

- ➢ Herstelwerkzaamheden: Voer de nodige herstelwerkzaamheden uit om het probleem op te lossen;
- ➢ Systemen herstellen: Breng getroffen systemen terug naar hun normale operationele status;
- ➢ Validatie: Bevestig dat alle herstelacties succesvol zijn uitgevoerd en dat het incident volledig is opgelost.

Wat doen we in de oefening:

- ☑ We stellen vast of we inzicht hebben in welke herstelacties gedaan moeten worden en wie die zou moeten uitvoeren;
- ☑ We stellen vast wie gemandateerd is voor deze herstelacties;
- ☑ We stellen vast hoe we kunnen valideren of de bedrijfsfuncties weer hersteld zijn;
- ☑ We stellen vast welke restpunten er nu nog open staan (zoals in de diagnose en eventueel het forensisch onderzoek).

8.2.3.7 Evaluatie (van het doorlopen incident en responseproces)

Wanneer: Na herstel.
Wat moet er gedaan worden:

- ➢ Evaluatie van de response: Evalueer de incidentresponse om te beoordelen hoe effectief de stappen waren;
- ➢ Identificatie van verbeterpunten: Identificeer hiaten en verbeterpunten in het proces;
- ➢ Documentatie van leerpunten: Documenteer de leerpunten en stel een verbeterplan op voor toekomstige incidenten.

Wat doen we in de oefening:

- ☑ We stellen vast of de informatie en documentatie die we gebruikt hebben nu voldoende waren voor de effectieve afhandeling;
- ☑ We stellen vast of de informatie over de melding, het incident en de betrokken assets voldoende en juist waren;
- ☑ We stellen vast of er geen informatie is verloren gegaan in de afhandeling;
- ☑ We stellen vast waar we te veel tijd verloren zijn in de afhandeling.

8.3 Evaluatie oefening & opvolging

In deze fase bespreekt de facilitator zijn bevindingen uit de tabletop-oefening. De evaluatie richt zich op het identificeren van sterke punten en verbeterpunten, en resulteert in specifieke actiepunten die het team moet opvolgen om de effectiviteit te vergroten.

8.3.1 Evaluatiecriteria

- ☐ Beoordeel de effectiviteit van de melding en de initiële response;
- ☐ Snelheid en duidelijkheid van communicatie;
- ☐ Besluitvormingsprocessen en hun kwaliteit;
- ☐ Evalueer de incidentoplossingsstappen;
- ☐ Evalueer de herstel strategieën.

8.3.2 Follow-up plan

- ☐ Opstellen van actiepunten voor verbeterpunten;
- ☐ Debriefing sessie met alle deelnemers;
- ☐ Implementatie van leerpunten in het incidentresponseplan en procedures;
- ☐ Evaluatie van impact van de scenario.

8.4 Resultaat tabletop oefening

De tabletop oefening heeft de volgende kernresultaten opgeleverd:

- ☐ Verbeterde classificatie: Het inzicht in de huidige classificatiecriteria voor incidenten is aanzienlijk verbeterd, waardoor er een gedetailleerde analyse kon worden gemaakt van de bestaande methoden. Aanbevelingen zijn geformuleerd om deze criteria te verfijnen, te standaardiseren en te integreren in een nieuw classificatiesysteem. Dit nieuwe systeem belooft een nauwkeurigere en consistentere incidentenclassificatie, wat essentieel is voor een efficiënte en effectieve response;
- ☐ Verhoogde samenwerking: De oefening heeft aangetoond dat verbeterde communicatie tussen teams cruciaal is voor een gecoördineerde en effectieve incidentresponse. Nieuwe en gedetailleerde protocollen zijn opgesteld om de samenwerking en informatie-uitwisseling tussen verschillende afdelingen te verbeteren. Deze protocollen omvatten specifieke communicatielijnen, frequenties van informatie-uitwisseling en escalatieprocedures, wat leidt tot een snellere reactie op incidenten;
- ☐ Identificatie van verbeterpunten: Gedurende de oefening zijn verschillende hiaten en inefficiënties in het huidige incidentresponseproces geïdentificeerd. Deze bevindingen zijn vertaald in gedetailleerde actiepunten, elk met toegewezen verantwoordelijken en strikte deadlines. De actiepunten omvatten zowel operationele als strategische verbeteringen, zoals de herstructurering van responseenheden, optimalisatie van hulpmiddelen en bijscholing van personeel, wat bijdraagt aan een algehele versterking van de incidentresponsecapaciteit;
- ☐ Verhoogd bewustzijn: De deelnemers hebben een dieper en genuanceerder inzicht gekregen in de uiteenlopende informatiebeveiligingsrisico's die de organisatie bedreigen. Op basis van deze inzichten zijn uitgebreide aanbevelingen gedaan voor gerichte training en bewustwordingsprogramma's, die specifiek zijn afgestemd op de verschillende niveaus binnen de organisatie. Deze programma's zijn ontworpen om het veiligheidsbewustzijn te vergroten en de medewerkers beter voor te bereiden op potentiële beveiligingsincidenten;
- ☐ Documentatie: Alle belangrijke discussies, beslissingen en leerervaringen zijn nauwgezet vastgelegd in een uitgebreid eindrapport. Deze documentatie biedt niet alleen een gedetailleerd overzicht van de oefening, maar dient ook als een waardevol naslagwerk voor toekomstige oefeningen. Het rapport bevat ook specifieke aanbevelingen voor continue verbetering en kan worden gebruikt als basis voor het bijwerken van beleidslijnen en procedures;
- ☐ Evaluatie van plannen: De bestaande incidentresponseplannen zijn grondig geëvalueerd en geanalyseerd tijdens de oefening. Op basis van de bevindingen zijn gedetailleerde voorstellen gedaan voor aanpassingen en verbeteringen. Deze voorstellen omvatten onder andere de herziening van escalatieprotocollen, de integratie van nieuwe technologieën voor incidentbeheer en de versterking van communicatiekanalen. Deze verbeteringen zijn essentieel om de responseplannen beter af te stemmen op de huidige dreigingsscenario's en de specifieke organisatorische behoeften, wat uiteindelijk resulteert in een robuustere en veerkrachtigere incidentresponse.

9 Tabletop III - Crisis escalatie oefening

Deze tabletop oefening richt zich op oefenen van een crisis escalatie. Dit houdt in dat er een crisis is binnen de organisatie, de oefening stopt wanneer er volgens het Business Continuity Plan met daarin het Crisis Management Plan er gede-escaleerd mag worden.

Voor het uitvoeren van de tabletop oefening volgen we het raamwerk beschreven in hoofdstuk 5 "Opzet van de oefeningen".

9.1 Voorbereidende fase

Tijdens de voorbereidende fase waarborgt de facilitator dat alle hulpbronnen beschikbaar zijn en dat alle zaken op de juiste wijze zijn geregeld.

9.1.1 Doelstellingen bepalen

Zie hoofdstuk 4.14.1 Doelstellingen voor het bepalen van de doelstelling voor de tabletop crisis escalatie oefening.

9.1.2 Deelnemers identificeren

De volgende deelnemers zijn benodigd bij een crisis escalatie.

- ☐ ISO van de organisatie;
- ☐ Leden van het crisismanagementteam;
- ☐ Juridische en compliance officers;
- ☐ Topmanagement;
- ☐ IT-personeel en applicatie, systeem- en netwerkbeheerders;
- ☐ Communicatieteam, belanghebbenden en derde partijen.

9.1.3 Scenario Kiezen

Voor het kiezen van een scenario maken we geen gebruik van het dobbelsteensysteem want nu hebben we een incident nodig wat gerelateerd is aan assets die bedrijfskritisch zijn voor de organisatie. Dit is nml. de meest gehanteerde criterium voor het uitroepen van een crisis.

9.1.4 Agenda ontwikkelen

Totale tijdsduur van scenario: 6 uur

In deze tijdsduur is er 1 uur en 40 minuten voorzien voor de activiteiten met pauzes die de oefening vorm geven (nr. 1, 2, 3, 6, 10 en 12) en 4 uren en 20 minuten voor het doorlopen van het scenario (nr. 3, 4, 5, 7, 8, 9 en 11). Voor deze 4,5 uren is een verwijzing naar de procesdoorloop activiteiten meegeven naast de tijdsindicatie).

Agenda:

1. Introductie, agenda, hulpbronnen uitgeven en basisregels bespreken (15 minuten)
2. Pre-oefenbriefing (15 minuten)
3. Uitvoeren processtap preparatie (30 minuten)
4. Uitvoeren processtap registratie & verificatie (30 minuten)
5. Uitvoeren processtap classificatie & prioritering (30 minuten)
6. Pauze (20 minuten)
7. Uitvoeren processtap onderzoek & diagnose (50 minuten)
8. Uitvoeren processtap containment (50 minuten)
9. Uitvoeren processtap oplossing & herstel (50 minuten
10. Pauze (20 minuten)
11. Uitvoeren processtap evaluatie incident (30 minuten)
12. Evaluatie oefening en opvolging (30 minuten)

9.1.5 Hulpbronnen verzamelen

- ☐ Beveiligingsincidentmanagement & response proces documentatie;
- ☐ Incidentmanagement procedures en -werkinstructies;
- ☐ Incidentresponseplannen (generiek en/of specifieke plannen);
- ☐ Communicatiebeleid en procedures;
- ☐ Documentatie over incidentoplossingen (Zie "Incident Response – Procesmodel (IR-4)");
- ☐ Contactinformatie van alle betrokkenen op basis van de gekozen assets;
- ☐ Toegang tot systeemlogs, data-analyse en monitoringtools;
- ☐ Crisismanagementplan (indien aanwezig).

9.1.6 Basisregels vaststellen

- ☐ Vertrouwelijkheid van de informatie waarborgen;
- ☐ Respect voor alle deelnemers en hun bijdragen;
- ☐ Focus op leren en verbeteren, niet op schuld toewijzen;

- ☐ Actieve deelname en constructieve feedback.

9.1.7 Voorbereiding van de facilitator

- ☐ De facilitator en eigenaar bepalen de doelstelling en kiezen een scenario met een incident en gerelateerde assets die zullen leiden tot een crisis-situatie;
- ☐ De facilitator zorgt ervoor dat alle hulpbronnen beschikbaar en aanwezig zijn;
- ☐ Zorg voor een veilige en rustige werkomgeving;
- ☐ Zorg ervoor dat alle deelnemers zijn geïdentificeerd en de oefening hebben geaccepteerd;
- ☐ Een interne senior IT-manager met ervaring in incidentbeheer;
- ☐ Een ervaren IT-manager met kennis van technische storingen;
- ☐ Voorgaande leerervaringen ophalen en hierop reflecteren;
- ☐ Follow-up meeting leiden en actiepunten concreet maken.

9.1.8 Technische opstelling

- ☐ Voorzien van presentatiemateriaal;
- ☐ Instellen van videoconferentietools voor deelnemers op afstand. (Indien het niet fysiek kan);
- ☐ Toegang tot relevante systemen en logs;
- ☐ Een rustige en ongestoorde ruimte voor de oefening.

9.2 Uitvoering tabletop oefening

Tijdens de tabletop-oefening worden de vooraf opgestelde scenario's uitgevoerd. Deze interactieve sessie biedt deelnemers de mogelijkheid om samen te werken, strategische beslissingen te nemen en potentiële reacties op incidenten te verkennen in een gesimuleerde omgeving.

9.2.1 Pre-oefenbriefing

- ☐ Uitleg van het doel, scenario, rollen en verantwoordelijkheden;
- ☐ Overzicht van de agenda;
- ☐ Verwachting omtrent actieve deelname en vertrouwelijkheid;
- ☐ Technische voorbereiding;
- ☐ Communicatielijnen oefenen.

9.2.2 Documenteer alles

- ☐ Gedetailleerde notities van alle onbeantwoorde vragen;
- ☐ Gedetailleerde notities van issues, acties en beslissingen die niet zijn ingevuld;
- ☐ Opname van de sessie voor latere analyse;
- ☐ Beslissingen en actiepunten vastleggen voor follow-up.

9.2.3 Processtappen voor incidentoplossing

Tijdens de crisis escalatie gaan we uit van een crisis, ook tijdens een crisis wordt hetzelfde pad als incident bewandelt.

9.2.3.1 1-Preparatie

Wanneer: Voorafgaand aan de afhandeling van het beveiligingsincident.
Wat moet er volgens het proces gedaan worden:

- Beschikbaarheid van incidentresponseplannen: Zorg ervoor dat gedetailleerde responseplannen beschikbaar zijn in hun huidige gepubliceerde versie;
- Rollen en verantwoordelijkheden: Zorg ervoor dat alle betrokkenen duidelijk weten wat hun rol en verantwoordelijkheden zijn in geval van een beveiligingsincident;
- Hulpmiddelen en technologie: Verzamel en test alle benodigde hulpmiddelen en technologieën om te verzekeren dat ze functioneel zijn tijdens de oefening.

Wat doen we in de oefening:

- ☑ We valideren of alle informatie die we nodig hebben aanwezig is en toegankelijk;
- ☑ of alle rollen uit het proces zijn ingevuld in de oefening;
- ☑ of alle communicatiemiddelen en andere hulpmiddelen aanwezig zijn en gebruikt kunnen worden.

9.2.3.2 2-Registratie en verificatie

Wanneer: Zodra een beveiligingsprobleem wordt gemeld.
Wat moet er gedaan worden:

- Documentatie van de melding als een beveiligingsincident: Gebruik een incidentregistratiesysteem om het incident gedetailleerd te documenteren. Gedetailleerd betekent hier conform de template van het registratiesysteem;
- Verificatie van het beveiligingsincident: Verifieer de authenticiteit van de melding van het beveiligingsprobleem met de beschikbare middelen;
- Stel vast of de melding daadwerkelijk valt binnen de te hanteren definitie van een securityincident;
- Bevestiging van betrokken asset: Identificeer de getroffen asset en stel vast wat de attributen zijn, waar het asset zich bevindt en wat aan de asset gerelateerd is (IT-systemen, data en bedrijfsprocessen).

Wat doen we in de oefening:

- ☑ We doorlopen de beschreven stappen conform de procesbeschrijving met gebruik van de tooling;
- ☑ We stellen vast dat iedereen de verantwoordelijkheid voor die processtap heeft genomen en dat dit van waarde was om die processtap effectief te doorlopen;

9.2.3.3 3-Classificatie & prioritering

Wanneer: Na registratie en verificatie van de beveiligingsmelding.
Wat moet er gedaan worden:

- Classificatie: Bepaal de ernst en impact van het incident op basis van de vooraf gedefinieerde criteria uit de procesbeschrijving en/of het beleid voor beveiligingsincident management en geef het incident de juiste classificering mee;
- Prioritering: Prioriteer het incident op basis van urgentie en de potentiële bedrijfsimpact;
- Responsestrategie: Stel een strategie op voor een snelle en effectieve response gebaseerd op de vastgestelde en geverifieerde classificatie en prioritering en de aanwezigheid van hierop beschreven beveiligingsincident- en responseplannen;
- Escalatie strategie: Bepaal of er hiërarchisch en technisch ge-escaleert moet worden. Een Hiërarchische escalatie moet plaats vinden als duidelijk is dat de impact van het incident binnen de definitie van een calamiteit waarvoor een crisis moet worden uitgeroepen valt.

Wat doen we in de oefening:

- ☑ We stellen vast of de aan het incident gerelateerde assets uit de assetregistratie te halen zijn en of die assets voldoende beschreven zijn om de impact op de bedrijfsvoering te kunnen inschatten en daarmee de classificatie van het beveiligingsincident;
- ☑ We stellen vast of de prioritering die het proces en de beleidsdocumenten geven aan dit incident voldoende is om de juiste snelheid in activiteiten en besluitvorming te realiseren;
- ☑ We stellen vast of we een specifieke of generieke beschrijving kunnen vinden om de afhandeling verder te kunnen voorzetten en indien niet aanwezig wordt die ter plekke geformeerd (zowel de strategie als de vervolgacties);
- ☑ We stellen vast of de huidige classificatie en urgentie al voldoende zekerheid geven om een crisis te laten uitroepen of dat er eerst nog diagnose moet plaatsvinden.

9.2.3.4 4-Onderzoek & diagnose

Wanneer: Na classificatie en prioritering.
Wat moet er gedaan worden:

- Gedetailleerd onderzoek: Voer een grondig onderzoek uit om de oorzaak van het incident te identificeren;
- Diagnose: Begrijp de omvang en impact van het incident door middel van forensisch onderzoek en analyse;
- Bewijsmateriaal verzamelen: Verzamel en documenteer bewijsmateriaal om de bevindingen te ondersteunen.

Wat doen we in de oefening:

- ☑ Deze activiteiten kunnen parallel plaatsvinden. Hoe verdelen we de aandacht?
- ☑ We doen een bepaling van de huidige omvang van het incident en de potentiële impact die het kan hebben op de betrokken assets en de bedrijfsvoering waar deze assets betrekking op hebben;
- ☑ We nemen in de bepaling van de impact het worst case scenario in ogenschouw en het meest waarschijnlijke scenario en we beperken ons niet tot onze eigen organisatie maar kijken naar de informatie en waardeketen waarin we gepositioneerd zijn;

- ☑ We bepalen of het vinden van de oorzaak en de wijze waarop dit incident heeft ontstaan nu zinvol is en prioriteit heeft, en hoe we kunnen zorgen dat er in ieder geval geen waardevolle informatie verloren gaat;
- ☑ We bepalen of de diagnose nu voldoende zekerheid geeft dat de (mogelijke) impact het uitroepen van een crisis rechtvaardigt;
- ☑ We bepalen ook of de diagnose voldoende zeker is om de impact (en daarmee ook de crisis) te kunnen rechtvaardigen. Indien nodig escaleren we technisch naar de leveranciers van de producten waarmee een relatie is waarin dat kan;
- ☑ We bepalen in samenwerking met het crisis management team welke informatie uit de diagnose zij nodig hebben die wij kunnen leveren om beslissingen te nemen over de communicatie naar de externe stakeholders en beslissingen over de bedrijfsvoering en het herstel zoals een complete technische en organisatorische uitwijk.

9.2.3.5 5-Containment

Wanneer: Zodra de eerste diagnose is voltooid.
Wat moet er gedaan worden:

- ➢ Maatregelen nemen: Neem onmiddellijk maatregelen om verdere schade te voorkomen en het incident in te dammen;
- ➢ Impact beperken: Beperk de impact van het incident op de bedrijfsvoering door getroffen systemen te isoleren;
- ➢ Communicatie: Informeer relevante stakeholders over de genomen stappen en de status van het incident.

Wat doen we in de oefening:

- ☑ We bepalen of de vooraf beschreven maatregelen uit de specifieke of generieke beschrijving voor securityincident response van toepassing en afdoende zijn en vullen dat aan waar we dat nodig vinden;
- ☑ We bepalen of het incident zich in een mogelijk af te schermen (netwerk) segmentatie voortdoet en of het mogelijk en zinvol is deze segmentering van de rest van onze organisatie af te schermen;
- ☑ We bepalen wie voor de isolatie verantwoordelijk is en of die gemandateerd is om dat besluit te mogen nemen. Omdat het inmiddels een crisis is zal de gemandateerde beschreven zijn in het Crisis Management Plan;
- ☑ Omdat het mandaat bij de deelnemers ontbreekt wordt contact gezocht met de gemandateerde uit het crisis management team om vast te stellen welke informatie die nodig heeft om deze beslissing te kunnen nemen;
- ☑ We bepalen hoe de response en containment acties (wat voor een belangrijk deel technisch van aard is) gaat samenwerken met het crisis management team (wat hiërarchisch van aard is).

9.2.3.6 6-Oplossing & herstel

Wanneer: Na containment. *Let op, in sommige gevallen kan het voorkomen dat de oplossing & herstel parallel met containment wordt uitgevoerd. Maar stapsgewijs komt oplossing & herstel na containment.*
Wat moet er gedaan worden:

- Herstelwerkzaamheden: Voer de nodige herstelwerkzaamheden uit om het probleem op te lossen;
- Systemen herstellen: Breng getroffen systemen terug naar hun normale operationele status;
- Validatie: Bevestig dat alle herstelacties succesvol zijn uitgevoerd en dat het incident volledig is opgelost.

Wat doen we in de oefening:

- ☑ We stellen vast of we inzicht hebben in welke herstelacties gedaan moeten worden en wie die zou moeten uitvoeren;
- ☑ We stellen vast wie gemandateerd is voor deze herstelacties;
- ☑ We stellen vast hoe we kunnen valideren of de bedrijfsfuncties weer hersteld zijn;
- ☑ We stellen vast in samenwerking met het crisis management team of we kunnen de-escaleren op basis van het herstel;
- ☑ We stellen vast welke restpunten er nu nog open staan (zoals in de diagnose en eventueel het forensisch onderzoek).

9.2.3.7 Evaluatie (van het doorlopen incident en responseproces)

Wanneer: Na herstel.
Wat moet er gedaan worden:

- Evaluatie van de response: Evalueer de incidentresponse om te beoordelen hoe effectief de stappen waren;
- Identificatie van verbeterpunten: Identificeer hiaten en verbeterpunten in het proces;
- Documentatie van leerpunten: Documenteer de leerpunten en stel een verbeterplan op voor toekomstige incidenten.

Wat doen we in de oefening:

- ☑ We stellen vast of de informatie en documentatie die we gebruikt hebben nu voldoende waren voor de effectieve afhandeling;
- ☑ We stellen vast of de informatie over de melding, het incident en de betrokken assets voldoende en juist waren;
- ☑ We stellen vast of we wisten bij wie en hoe we de crisis konden initiëren;
- ☑ We stellen vast of we op het juiste moment hebben geëscaleerd;
- ☑ We stellen vast of de processen van incident response en crisis management op een adequate manier hebben samengewerkt en gecommuniceerd;
- ☑ We stellen vast of we de communicatie en samenwerking met de leveranciers hebben kunnen beheersen;
- ☑ We stellen vast of er geen informatie is verloren gegaan in de afhandeling;

- ☑ We stellen vast waar we te veel tijd verloren zijn in de afhandeling.

9.3 Evaluatie oefening & opvolging

In deze fase bespreekt de facilitator zijn bevindingen uit de tabletop-oefening. De evaluatie richt zich op het identificeren van sterke punten en verbeterpunten, en resulteert in specifieke actiepunten die het team moet opvolgen om de effectiviteit te vergroten.

9.3.1 Evaluatiecriteria

- ☐ Beoordeel de effectiviteit van de melding en de initiële response;
- ☐ Snelheid en duidelijkheid van communicatie;
- ☐ Besluitvormingsprocessen en hun kwaliteit;
- ☐ Evalueer de incidentoplossingsstappen;
- ☐ Evalueer de herstel strategieën.

9.3.2 Follow-up plan

- ☐ Opstellen van actiepunten voor verbeterpunten;
- ☐ Debriefing sessie met alle deelnemers;
- ☐ Implementatie van leerpunten in het incidentresponseplan en procedures;
- ☐ Evaluatie van impact van de scenario.

9.4 Resultaat tabletop oefening

De tabletop oefening heeft de volgende kernresultaten opgeleverd:

- ☐ Verbetering van crisiscommunicatie: Tijdens de oefening zijn gedetailleerde en robuuste protocollen voor interne en externe communicatie ontwikkeld en aangescherpt. Deze protocollen zijn ontworpen om te functioneren onder verschillende escalatieniveaus, waardoor teams in staat zijn om zelfs onder hoge druk snel en nauwkeurig informatie uit te wisselen. Dit leidt tot een verkorting van reactietijden en een aanzienlijke verbetering van de responsecoördinatie;
- ☐ Versterking van teamcohesie en samenwerking: De oefening heeft gezorgd voor een diepgaande herziening van de rollen en verantwoordelijkheden van teamleden tijdens een crisissituatie. Er is nu een helder inzicht in wie welke acties moet ondernemen, zelfs in complexe en snel escalerende crisis. Deze duidelijkheid heeft de samenwerking tussen verschillende afdelingen en teams verbeterd, wat heeft geresulteerd in een meer geïntegreerde en strategische aanpak van crisisbeheer;
- ☐ Effectieve besluitvorming: De besluitvormingsprocessen zijn grondig geëvalueerd en verfijnd met het oog op crisis escalatie. Er zijn methoden geïdentificeerd om deze processen te optimaliseren, inclusief het betrekken van de juiste stakeholders bij verschillende escalatieniveaus. Dit zorgt ervoor dat teams beter voorbereid zijn om snel, goed onderbouwde beslissingen te nemen op basis van real-time informatie en veranderende omstandigheden, wat cruciaal is tijdens een escalerende crisis;
- ☐ Herkenning van knelpunten en verbeterpunten: De oefening heeft diepgaande inzichten verschaft in de zwakke punten van het huidige processen en communicatiestrategieën. Deze knelpunten zijn nauwkeurig geïdentificeerd en vertaald in specifieke, uitvoerbare aanbevelingen en actiepunten. Deze actiepunten zijn ontworpen om systemische inefficiënties te elimineren;
- ☐ Toegenomen paraatheid en responsecapaciteit: Deelnemers hebben tijdens de oefening ervaring opgedaan met het omgaan met uiteenlopende crisisscenario's en escalatieniveaus. Dit heeft hun paraatheid en vermogen om effectief te reageren op crisis aanzienlijk vergroot. Daarnaast zijn er responsestrategieën ontwikkeld die flexibel genoeg zijn om te worden toegepast op diverse toekomstige crisissituaties, waardoor de organisatie beter gepositioneerd is om onverwachte gebeurtenissen te beheersen;
- ☐ Documentatie en rapportage: Alle belangrijke discussies, beslissingen en leerervaringen zijn nauwgezet en vastgelegd in een uitgebreide documentatie. Deze documentatie biedt niet alleen een waardevol naslagwerk, maar dient ook als een strategisch hulpmiddel voor toekomstige oefeningen. Het rapport bevat een uitgebreide analyse van de resultaten, inclusief sterke en zwakke punten (SWOT-analyse), en biedt diepgaande aanbevelingen voor continue verbetering en vervolgstappen;
- ☐ Verhoogd bewustzijn en training: De oefening heeft geleid tot een verhoogd bewustzijn onder medewerkers en hun specifieke rol in een escalatiescenario. Op basis van deze bevindingen zijn er gerichte bewustwordingscampagnes en trainingsprogramma's ontwikkeld. Deze programma's zijn specifiek ontworpen om teamleden beter voor te bereiden op de complexe dynamiek van crisis escalatie, door hen te voorzien van de nodige vaardigheden en kennis;
- ☐ Naleving van regelgeving en beleid: Waar nodig zijn beleid en procedures aangepast om te voldoen aan wettelijke vereisten en best practices in crisismanagement. Deze aanpassingen zorgen ervoor dat de organisatie niet alleen juridisch compliant is, maar ook operationeel robuust en voorbereid op complexe crisisomstandigheden.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl

Juli 2025