TLP:GREEN

IR-4 PROCESMODEL

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	Doelgroep
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.	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	20-06-2025	Initiële versie
V1.1	30-6-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Incident Response – Procesimplementatie	Zie "IR-4, Incident Response – Procesimplementatie (pdf)" onder Incident Response Readiness
Incident Response – Capability Assessment	Zie "IR-1, Incident Response – Capability Assessment" onder Incident Response Readiness
Incident Response Readiness miniproducten	Zie Incident Response Readiness op ncsc.nl
Baseline Informatiebeveiliging Overheid v1.04zv	https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf
NIST-CSF 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
Besluit CIO-stelsel Rijksdienst 2021	https://wetten.overheid.nl/BWBR0044613/2021-01-01
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.

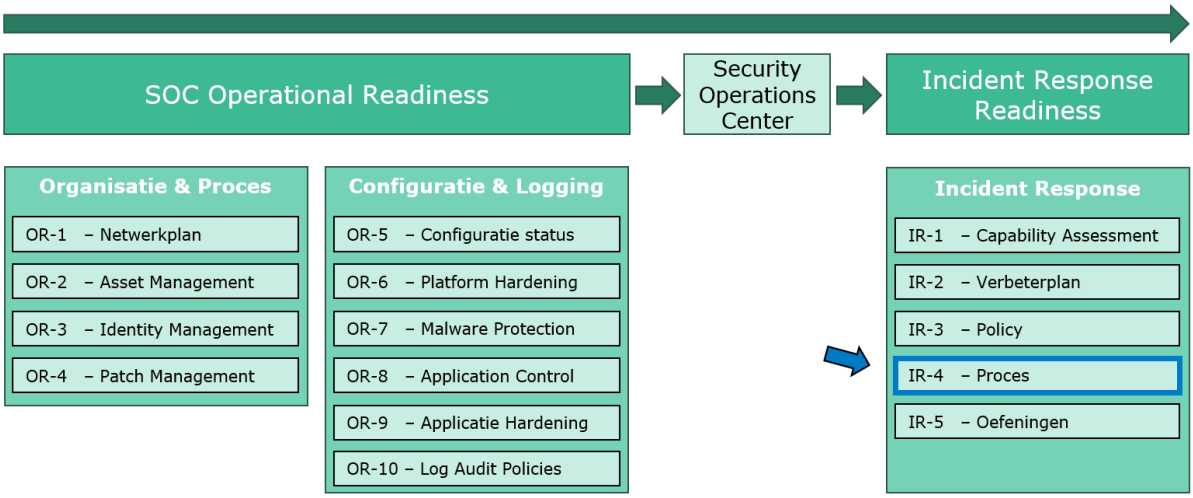
2 Context miniproducten

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 security melding 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-4 Proces bestaan uit:

- Procesmodel (**Dit document**)
  PDF document voorziet in het procesmodel voor Incident Response

- Procesimplementatie
  PDF document voorziet in de implementatie van het procesmodel Incident Response

3 Leeswijzer

Deze leeswijzer helpt je bij het effectief gebruiken van dit document en het correct toepassen van het procesmodel.

3.1 Voorbereiding

Voordat je dit document gebruikt:

- Zorg dat je het 'Capability Assessment (IR-1)' ten minste voor het thema proces hebt uitgevoerd. Dit helpt om de huidige situatie van je organisatie te bepalen en de juiste verbeteracties te selecteren.

3.2 Structuur van dit document

Dit document maakt geen onderscheid in niveaus. Zoals beschreven in het 'Capability Assessment (IR-1)' is er vanaf niveau 1 een specifiek proces voor beveiligingsincidenten ingericht.

In paragraaf 4.3 is het procesmodel gevisualiseerd. In de onderliggende paragraven is elke processtap verder uitgewerkt. In paragraaf 4.4 en onderliggende paragraven zijn rollen, taken, bevoegdheden en verantwoordelijkheden beschreven.

3.3 Wat is het doel van dit document?

Dit document helpt je om binnen de context van informatiebeveiliging:

- (Nieuwe) Incident Response processen te toetsen met het organisatie beleid;
- Bestaande processen te toetsen op volledigheid en waar nodig uit te breiden;
- Ondersteuning ter voorbereiding op de procesimplementatie met behulp van het kennisdocument 'Procesimplementatie (IR-4)';
- Het inrichten van processen volgens het hier beschreven model helpt organisaties om te voldoen aan eisen vanuit de Baseline Informatiebeveiliging Overheid (BIO) en de NIS2-richtlijn.

3.4 Gebruik van dit document

Dit document bevat een beschrijving van een procesmodel voor de response op beveiligingsincidenten. Je kunt het document op verschillende manieren gebruiken, afhankelijk van je doel:

- Startpunt bij het inrichten van het beveiligingsincident- & responseproces;
- Toets bestaande Incident Response processen.

Aanvullend op dit document kan het document 'Procesimplementatie (IR-4)' worden gebruikt ter ondersteuning van de implementatie van het procesmodel uit dit document.

4 Beveiligingsincident- & responsemanagement

4.1 Inleiding

Dit document bevat een beschrijving van een procesmodel voor de response op beveiligingsincidenten dat als startpunt kan dienen bij het inrichten van het beveiligingsincident- & responseproces, waarbij de opgenomen elementen worden beschouwd als het minimum dat in een beleid moet worden opgenomen.

Als essentieel onderdeel van het incident- & responsemanagement, dient de organisatie verantwoordelijkheden, controles en procedures te implementeren die een snelle, doeltreffende en ordelijke response op informatiebeveiligingsincidenten mogelijk maken. Het primaire doel is het minimaliseren van de impact van incidenten aan de bedrijfsvoering en/of maatschappij.

4.2 Procesvoorbereidingen

Beschrijving:
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. Deze scenario's resulteren in responseplannen. Wij adviseren om de responseplannen volgens de PDCA-cyclus (jaarlijks) te reviewen en te actualiseren als uit de evaluatie van een kritisch beveiligingsincident blijkt dat het bestaande responseplan niet voldoet.

Doel:
Door vooraf gestructureerd de activiteiten te beschrijven die genomen moeten worden bij melding van een beveiligingsincident, kan sneller en effectiever worden gereageerd met als doel impactreductie. Het voorkomt ook dat tijd en energie verloren gaat aan acties die dit doel niet bereiken.

Input:
- Informatiebeveiligingsbeleid
- Dreigingsanalyse die aangeeft:
    - Wat de meest voor de hand liggende aanvallers zijn.
    - Wat de aanvalsmethoden voor cyberaanvallen zijn.
    - Wat de te beschermen belangen zijn.
- Informatiebeveiligingsrisicoanalyse die aangeeft waar de kwetsbaarheden liggen in de organisatie.
- Best practices (bijvoorbeeld de door het NCSC gepubliceerde responseplannen).
- Evaluaties van eerdere beveiligingsincidenten.
- Eerdere versies van responseplannen.
- Beveiligingsincident- en responsebeleid.
- Scenario's voor containment, verwijdering en herstel.

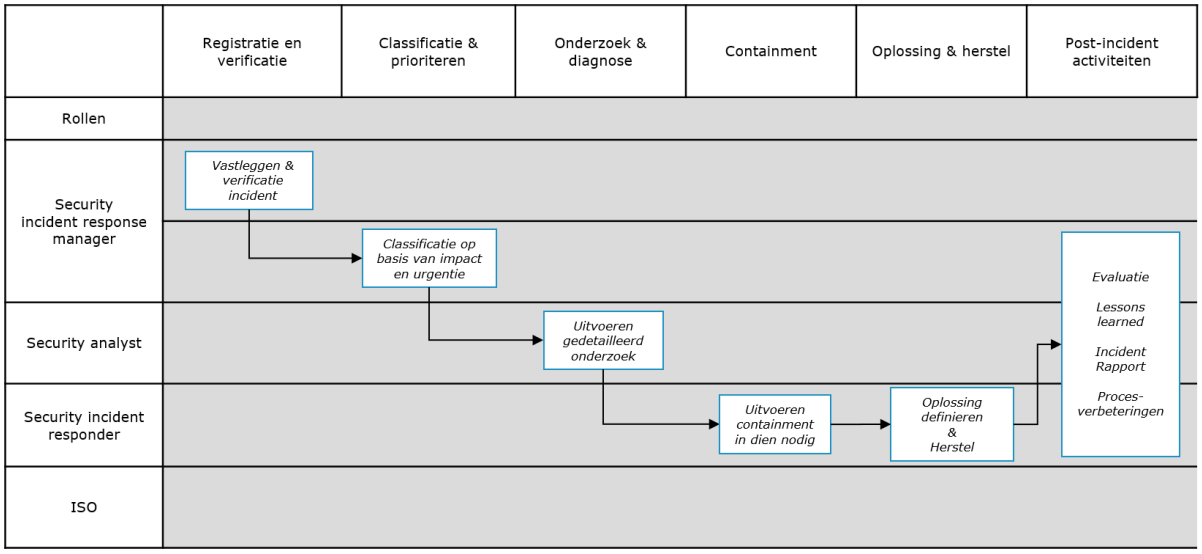
Activiteiten:
- Creatie van een nieuw of geactualiseerd algemeen responseplan op basis van het beleid, best practices, leermomenten van eerdere incidenten bij de eigen en gelijksoortige organisaties en de belangrijkste dreigingen voor de organisatie.

- Creatie van een nieuw of geactualiseerd specifiek responseplan voor scherp af te bakenen beveiligingsincidenten die een specifieke response rechtvaardigen.

Output:
- Een generiek informatie beveiligings- en responseplan (bijvoorbeeld hoe en wanneer leveranciers en/of afnemers te betrekken).
- Een bijgewerkt specifieke beveiligings- en responseplan.

4.3 Beveiligingsincident & responseproces

Onderstaande flowchart biedt een visueel overzicht van het beveiligingsincident- & responseproces. In de rijen staan de betrokken rollen weergegeven en in de kolommen de verschillende processtappen die geïdentificeerd zijn. De vermelde processtappen preparatie en containment maken het beveiligingsincident- & responseproces onderscheidend ten opzichte van het reguliere incident & -responseproces.



Figuur 1 Flowchart Beveiligingsincident- & responseproces

Hieronder worden de processtappen uit de flowchart in meer detail beschreven.

In de paragrafen 4.3.3 en 4.3.5 wordt bij escalatie verwezen naar de processen "business continuity management" en crisismanagement. Deze worden niet verder in detail besproken, aangezien het uitgangspunt is dat deze processen reeds zijn ingericht.

4.3.1 Registratie & verificatie data

Beschrijving:
De melding van een mogelijk beveiligingsincident wordt bij binnenkomst door de Security incident- en responsemanager vastgelegd in het ticketsysteem. 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. Het resultaat van de verificatie kan ook zijn dat de melding ten onrechte was aangemerkt als een beveiligingsincident waardoor het kan worden afgesloten.

Doel:
Het doel is om het gemelde beveiligingsincident systematisch te registreren en de documentatie te verifiëren zodat het effectief gevolgd en opgevolgd kan worden. Het registreren en verifiëren met een ticketsysteem, ondersteunt het stroomlijnen van de communicatie voor een juiste en volledige opvolging door de verschillend betrokken rollen. Hierdoor wordt de controle behouden en geborgd, zodat de organisatie zich kan focussen op een oplossing.

Input:
- Meldingen van mogelijke beveiligingsincidenten (vanuit gebruikers, SOC, monitoringsystemen, etc.).
- Basisinformatie over de melding (beschrijving, tijdstip, initiële impact).

Activiteiten:
- Registreren van melding gegevens in het ticketsysteem.
- Verifiëren van de melding waarbij aan de hand van criteria de initiële risico's en impact worden vastgesteld.
- Vastleggen van de initiële risico's en impact.
- Bepalen van de urgentie op basis van de vastgestelde initiële risico's en impact.
- Als uit verificatie blijkt dat het gemelde beveiligingsincident geen risico's en impact heeft, kan de melding worden afgesloten inclusief (indien van toepassing) een terugkoppeling aan de melder.

Output:
- Een geregistreerd beveiligingsincident, inclusief relevante gegevens en details.
- Óf: Een afgesloten melding als uit verificatie blijkt dat de melding geen risico en of impact oplevert, en het daarom geen beveiligingsincident betreft.

4.3.2 Bepalen impact, urgentie, prioriteit

Beschrijving:
Beveiligingsincidenten worden vaak ingedeeld in hardware-, software-, of netwerk categorieën waardoor duidelijk wordt welk oplosteam de vervolgstap onderzoek & diagnose gaat oppakken. Het beveiligingsincident wordt geanalyseerd waarbij op basis van impact en urgentie een prioriteit wordt vastgesteld. Deze prioriteit is bepalend voor de snelheid en voorrang in de toewijzing van mensen middelen die worden ingezet om de oorzaak weg te nemen en zo te voorkomen dat het beveiligingsincident verder wordt geëxploiteerd.

Doel:
Het doel is om het beveiligingsincident correct te prioriteren en classificeren. Dit zorgt voor een efficiënte en optimale inzet van mensen en middelen, waarbij de totaal impact van alle beveiligingsincidenten tezamen, optimaal wordt gemanaged.

Input:
- Een geregistreerd beveiligingsincident in het ticketsysteem, inclusief alle noodzakelijke details.

Activiteiten:
- Beveiligingsincidenten worden geprioriteerd op basis van vastgestelde impact en urgentie. Een voorbeeld van een inschalingskader (oftewel classificatie) voor impact en urgentie is als volgt:

  Impact-bepaling:
  - Kritiek: Ernstige impact op bedrijfsvoering en gegevensbeveiliging en/of de organisatie kan niet aan haar wettelijke taken en verplichtingen voldoen.
  - Hoog: Aanzienlijke verstoring op bedrijfsvoering of gegevens corrumpering.
  - Gemiddeld: Matige impact met beperkte gegevensblootstelling
  - Laag: Minimale impact op systemen of gegevens

  Urgentie-bepaling:
  - Hoge urgentie: Er vindt momenteel exploitatie plaats. Het beveiligingsincident heeft een directe impact op de organisatie, waardoor onmiddellijke actie vereist is om verdere schade of verlies te voorkomen
  - Gemiddelde urgentie: verwachting van exploitatie op korte termijn. Hoewel er op dit moment geen actieve exploitatie is, zijn er aanwijzingen of kwetsbaarheden die suggereren dat een aanval waarschijnlijk is.
  - Lage urgentie: Dit niveau van urgentie duidt aan dat er geen indicaties zijn voor mogelijke exploitatie. De incidenten op dit niveau hebben een minimale impact op de organisatie en kunnen met minder urgentie worden behandeld.

- Op basis van de inschaling van impact en urgentie wordt de prioriteit bepaald.
- Het beveiligingsincident wordt ook naar type dreiging geclassificeerd (bijvoorbeeld malware, phishing, DdoS-aanvallen, insider threat etc.).

Output:
- Geclassificeerd en geprioriteerd beveiligingsincident.
- Duidelijke richtlijnen voor de vervolgactiviteiten, gegeven de classificatie en prioriteit.

4.3.3 Uitvoering gedetailleerd onderzoek

Beschrijving:
In deze fase vindt nader onderzoek plaats, om de oorzaak van het beveiligingsincident te achterhalen en werkelijke impact te valideren. Dit omvat onder meer het analyseren van aanwezige systeemlogs, netwerk-architectuur, configuratie-informatie en overig beschikbare technische gegevens. Tevens worden maatregelen genomen om verdere impact te minimaliseren en herhaling in de toekomst te voorkomen.

Doel:
Het doel is om de oorzaak van het beveiligingsincident te identificeren en te begrijpen hoe het beveiligingsincident heeft kunnen ontstaan, wat de impact is, hoe de schade door mogelijke verspreiding is te beperken en daarmede de impact onder controle te krijgen.

Input:
- Geclassificeerd en geprioriteerd beveiligingsincident.
- Relevante netwerk- en systeeminformatie zoals logs, systeemdata, architectuur en netwerkverkeer.
- Aanwezige beveiligingsmaatregelen zoals firewall- en toegangsregels of de status van antivirus en anti-malware.
- De responseplannen welke in de preparatiefase zijn voorbereid

Activiteiten:
- Het selecteren van relevant(e) responseplan(nen).
- Analyseren van systeemlogs, netwerkverkeer en andere relevante gegevens om de oorzaak van het beveiligingsincident vast te stellen.
- Het identificeren van (potentiële) kwetsbaarheden en/of dreigingen.
- In het geval de lijnorganisatie (de rollen zoals benoemd in het proces) concludeert dat de scope van de schade dusdanig groot is dat een tijdelijke oplossing door hen niet tijdig en effectief kan worden uitgevoerd, dient geëscaleerd te worden naar het proces “crisismanagement”

Output:
- Een (gedetailleerd) rapport over de oorzaak en werkelijke impact van het beveiligingsincident.
- Maatregelen ter voorkoming van herhaling van het beveiligingsincident
- Voorlopige bevindingen voor herstel.
- Relevant(e) responseplan(nen)

4.3.4 Uitvoering containment

Beschrijving:
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. Dit kan door het implementeren van tijdelijke maatregelen, door het inperken of isoleren van de omgeving waarbinnen het beveiligingsincident is opgetreden of door het toepassen van maatregelen die ervoor zorgen dat de impact en/of risico niet verder kan escaleren zonder noodzakelijkerwijs alles volledig te isoleren. Snelheid is hierbij van belang. Denk bijvoorbeeld aan moderne malware die zichzelf zal verspreiden in de omgeving en waarbij de werking van malware ook zal doorwerken in gebieden die nog niet besmet zijn.

In de responseplannen is vooraf gedefinieerd voor welke type beveiligingsincidenten welke wijze van containment van toepassing is, inclusief de benodigde mandaten voor welke rol wat mag beslissen. Dit kan bijvoorbeeld door het verbreken van de connectie tussen verschillende netwerkdomeinen of door het geheel of gedeeltelijk stoppen van de levering van IT-diensten. In

het uiterste geval vindt containment plaats door het volledig uitschakelen van alle IT-infrastructuur.

Niet alle scenario's zullen uitgaan van een containment, met name wat lager geclassificeerde beveiligingsincidenten waar nog geen exploitatie van een kwetsbaarheid is geconstateerd kennen niet standaard een containment.

Doel:
Het doel is om de impact van een beveiligingsincident te beperken en te beheersen zodat verdere verspreiding of escalatie wordt voorkomen. De dreiging dient onder controle te worden gehouden, waarbij de bedrijfsvoering zo veel mogelijk wordt voortgezet.

Input:
- Gedetailleerd rapport over de oorzaak van het beveiligingsincident en de gevolgen.
- Relevante netwerk en systeem informatie zoals logs, systeemdata, architectuur en netwerkverkeer.
- Beveiligingsmaatregelen zoals firewall- en toegangsregels of de status van antivirus en anti-malware.
- Relevant(e) responseplan(nen)

Activiteiten:
- Analyse van de mogelijkheden om de oorzaak van kwetsbaarheden en de gevolgen van het beveiligingsincident te beperken.
- Analyse van de toepasselijkheid van de bestaande responseplannen.
- Uitvoeren en rapporteren van de containment activiteiten.
- Implementeren van tijdelijke maatregelen om verdere schade te voorkomen.
- Het opheffen van tijdelijke maatregelen en containment.
- Communiceren naar de gebruikersorganisatie en andere belanghebbenden over de consequenties van de te nemen acties

Output:
- Rapportage containment acties en consequenties

4.3.5 Bepalen oplossing, implementeren herstel

Beschrijving:
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. Gebruikers en andere belanghebbenden, waaronder bijvoorbeeld informatie-eigenaren, worden ook op de hoogte gebracht over de voortgang van de oplossing van het beveiligingsincident.

Doel:
Het doel van deze fase is om een veilige werking van de IT-systemen te herstellen door het toepassen van permanente oplossingen en herstelmaatregelen. Het herstellen van de IT-systemen en het verhelpen van de onderliggende oorzaken zorgt ervoor dat het beveiligingsincident volledig wordt opgelost en zich niet herhaalt.

Input:
- Diagnose en bevindingen uit de fase Onderzoek & Diagnose.
- Rapportage over de genomen (tijdelijke) maatregelen in het containment proces

Activiteiten:
- Eradicatie (uitroeiing) van de oorzaak van het beveiligingsincident
- Bepalen en implementeren van (meer) permanente oplossingen (bijvoorbeeld wegnemen kwetsbaarheden via beveiliging patches, updaten van configuraties etc.).
- Volledig herstellen van de beschikbaarheid van IT-systemen en gecorrumpeerde gegevens. In geval de lijnorganisatie (de rollen zoals benoemd in het proces) concludeert dat de (scope van de) schade dusdanig groot is dat herstel niet door hen tijdig en effectief kan worden

uitgevoerd, dient geëscaleerd te worden naar het proces "Business Continuity Management" van waaruit geëscaleerd kan worden naar "Crisis management".
- Testen van de IT-systemen na herstel om te verzekeren dat de problemen zijn opgelost en het veiligheidsniveau is hersteld.
- Eventueel genomen tijdelijke maatregelen opheffen zodra de permanente oplossing is geïmplementeerd.

Output:
- De herstelde normale beschikbaarheid en werking van de IT-systemen en gegevens, bijvoorbeeld doordat kwetsbaarheden zijn gepatcht, gecorrumpeerde gegevens zijn hersteld en/of hardware is vervangen.
- Documentatie van alle stappen uit het incidentmanagement en -reponseproces.
- Geïnformeerde stakeholders via communicatie en rapportage.

4.3.6 Post-incident activiteiten

Beschrijving:
Nadat het beveiligingsincident is opgelost moeten de volgende activiteiten plaatsvinden.

Opstellen incidentrapport
Het incidentrapport voorziet in een managementsamenvatting en is input voor de evaluatie.

Evaluatie met alle betrokkenen
De evaluatie is input voor het proces, detectie-algoritmen en use-cases.

Lessons learned
Voor structurele verbetering worden de lessons learned verwerkt in het beveiligingsincident- & responseproces, en in het bijzonder de responseplannen. Het doel is om de effectiviteit, schaalbaarheid en snelheid van processen te verbeteren, zodat toekomstige beveiligingsincidenten sneller en beter kunnen worden aangepakt.

Procesverbeteringen
Dit omvat ook het reguliere incidentbeheerproces en het aanpassen van beleid of procedures, waar nodig.

Doel:
Het doel is om als organisatie te leren van het beveiligingsincident en de weerbaarheid van de organisatie qua IT-systemen en processen te vergroten. De evaluatie draagt bij aan het optimaliseren van incidentresponsestrategieën.

Input:
- Beveiligingsincident documentatie van alle doorlopen stappen uit het incident- & responseproces;
- Herstelmaatregelen en de effectiviteit van de genomen acties;
- Gegevens (gemeten KPI's) over de incidentresponse voor en na toepassing van permanente oplossingen uit de fase Oplossing & Herstel;
- Feedback van de belangrijkste stakeholders.

Activiteiten:
- Opstellen incident rapportage;
- Evalueren van de genomen response- en herstelmaatregelen om te bepalen welke effectief en efficiënt waren en welke alsnog verbetering behoeven;
- Documenteren van verbeterpunten en het aanpassen van beleid, procedures en processen;
- Het doen van voorstellen aan detectie ter optimalisatie van bestaande en/of nieuwe use-cases en/of detectie drempelwaarden, waar van toepassing;
- Implementeren van operationele en tactische verbeteringen.

Output:
- Incident rapport;
- Evaluatierapport met conclusies en beveiligingsverbeterpunten om toekomstige beveiligingsincidenten te voorkomen;
- Aangepaste processen en beleidsaanpassingen, waar van toepassing;
- Terugkoppeling van bevindingen naar het SOC, Helpdesk, medewerkers, etc., onder meer voor het optimaliseren van detectie use-cases.

4.4 RACI Matrix en rolbeschrijvingen

4.4.1 Beschrijving

Hieronder is de RACI-matrix voor alle bovengenoemde processtappen van de flowchart beschreven.

	Security incident- en response manager	Security analist	Security incident responder	ISO	CISO
Registratie & Verificatie	**A, R**	**I**	**I**	**I**	**I**
Classificeren & Prioriteren	**A, R**	**C**	**I**	**I**	**I**
Onderzoek & diagnose	**A**	**R**	**R**	**I**	**I**
Containment	**A**	**C**	**R**	**C**	**I**
Oplossing & herstel	**A**	**C**	**R**	**I**	**I**
Post-incident activiteiten	**A**	**R**	**R**	**R**	**I**

Tabel 1 RACI Matrix

Een RACI-model is een hulpmiddel voor het definiëren van rollen en verantwoordelijkheden binnen een project of proces. Het staat voor:

R (Responsible): Degene die verantwoordelijk is voor de uitvoering van een taak of activiteit. Dit is de persoon die het werk uitvoert.
A (Accountable): Degene die eindverantwoordelijk is. Deze persoon zorgt ervoor dat de taak correct en tijdig wordt uitgevoerd en geeft goedkeuring.
C (Consulted): Personen of teams die geraadpleegd worden voor hun input of expertise. Dit zijn vaak belanghebbenden die adviseren.
I (Informed): Personen of teams die geïnformeerd moeten worden over de voortgang of resultaten, maar geen directe betrokkenheid hebben.

4.4.2 Rolbeschrijvingen

Hier wordt de rolbeschrijving verder uitgewerkt, evenals de belangrijkste verantwoordelijkheden van de rol.

4.4.2.1 Security incident- en response manager (SIRM)

Beschrijving:
Verantwoordelijk voor het end-to-end coördineren, beheren en leiden van de reactie op beveiligingsincidenten binnen de organisatie. Deze rol heeft als doel de impact van beveiligingsincidenten te minimaliseren en de kwaliteit en beschikbaarheid van de IT-dienstverlening snel te helpen herstellen. De SIRM zorgt voor een gestructureerde aanpak van beveiligingsincidenten en werkt nauw samen met andere teams en rollen waaronder incident responders en Security analisten, om beveiligingsincidenten effectief aan te pakken.

Belangrijkste verantwoordelijkheden:
- Registreren van beveiligingsincidenten in het incidentmanagementsysteem en zorgen voor verificatie en gedetailleerde documentatie van het beveiligingsincident.
- Classificeren en prioriteren van beveiligingsincidenten op basis van impact en urgentie.
- Rapporteren van de voortgang van beveiligingsincidenten aan het management en andere belanghebbenden.
- Ondersteunen van het technische onderzoek door de Security analist naar de oorzaak van beveiligingsincidenten en het vaststellen van de benodigde herstelmaatregelen.
- Coördineren van de response op beveiligingsincidenten.
- Begeleiden van de post-incident evaluatie en het vaststellen van verbeterpunten voor toekomstige beveiligingsincidenten.

4.4.2.2 Security analist

Beschrijving:
De Security analist is een specialist op het gebied van IT-beveiliging die diepgaande kennis heeft van potentiële dreigingen en van de technieken om systemen en data te beschermen. Deze onderzoekt de oorzaak van beveiligingsincidenten en ondersteunt bij het oplossen ervan.

Belangrijkste verantwoordelijkheden:
- Voeren van analyses van beveiligingsincidenten om de oorzaak en de impact te achterhalen.
- Adviseren over beveiligingsmaatregelen en oplossingen, zoals patches of configuratiewijzigingen, om het beveiligingsincident op te lossen.
- Adviseren bij het implementeren van mitigatie- en herstelmaatregelen om de schade te beperken en de veilige werking van informatievoorzieningen te herstellen.
- Verstrekken van technische expertise bij het oplossen van complexe beveiligingsincidenten.

4.4.2.3 Security incident responder

Beschrijving:
De Security incident responder is verantwoordelijk voor (het toezien op) de uitvoering van het herstel van IT-systemen en het verhelpen van de gevolgen van een beveiligingsincident. Deze werkt samen met de Security analist om te zorgen voor een snelle en efficiënte oplossing van het beveiligingsincident.

Belangrijkste verantwoordelijkheden:
- Assisteren van systeemeigenaren binnen beheerorganisatie bij het implementeren van tijdelijke en permanente herstelmaatregelen om het beveiligingsincident op te lossen.
- Beheren van de communicatie met interne en externe belanghebbenden over de voortgang van het beveiligingsincident.
- Documenteren van de genomen acties en de effectiviteit van de herstelmaatregelen.
- Ervoor zorgen dat de technische oorzaken van het beveiligingsincident volledig zijn weggenomen waarbij de uitvoering hiervan kan worden gedaan door de beheerorganisatie.

4.4.2.4 CISO (Chief Information Security Officer)

Beschrijving:
De CISO is de hoogst verantwoordelijke voor advies, kaderstelling en controle op beveiliging. Deze rol zorgt ervoor c.q. ziet erop toe dat het beheer op beveiligingsincidenten adequaat wordt uitgevoerd.

Belangrijkste verantwoordelijkheden:
- Eindverantwoordelijkheid voor de algehele beveiligingsstrategie van de organisatie, inclusief het beveiligingsincident- & responseproces.
- Zorg dragen voor de evaluatie van beveiligingsincidenten op tactisch niveau en bepalen of er beleidsaanpassingen nodig zijn.
- Toezicht houden op het beveiliging incidentbeheer en zorgen voor de implementatie van verbeteringen op basis van evaluaties.
- Het management over beveiligingsrisico's en de noodzaak van veranderingen in het beveiligingsbeleid.

4.4.2.5 ISO (Information Security Officer)

Beschrijving:
De ISO is verantwoordelijk voor het waarborgen van de informatiebeveiliging binnen de organisatie. Deze rol houdt toezicht op het ontwikkelen, implementeren en onderhouden van het informatiebeveiligingsbeleid en de procedures, en zorgt ervoor dat de organisatie voldoet aan de relevante wet- en regelgeving. De ISO speelt een sleutelrol bij het managen van risico's en het beschermen van bedrijfsgegeven. Bij kleinere organisaties waar geen capaciteit is om de werkzaamheden bij meerdere personen te beleggen, kan deze ISO-rol worden gecombineerd met de CISO-rol.

Belangrijkste verantwoordelijkheden:
- Adviseren van het management over informatiebeveiligingskwesties, risicomanagement en strategieën om de beveiliging te verbeteren.
- Het deelnemen aan en het verbeteren van post-incident evaluaties en het implementeren van verbetermaatregelen op basis van eerdere evaluaties, dreigingsanalyses en responseplannen.
- Het uitvoeren van de jaarlijkse informatiebeveiligingsmanagement systeem (ISMS).

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 (Rijksoverheid)

Juni 2025