TLP:GREEN

IR-4 PROCESIMPLEMENTATIE

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

1.2 Referenties

Document	Link
Incident Response – Procesmodel	Zie "IR-4, Incident Response – Procesmodel (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.

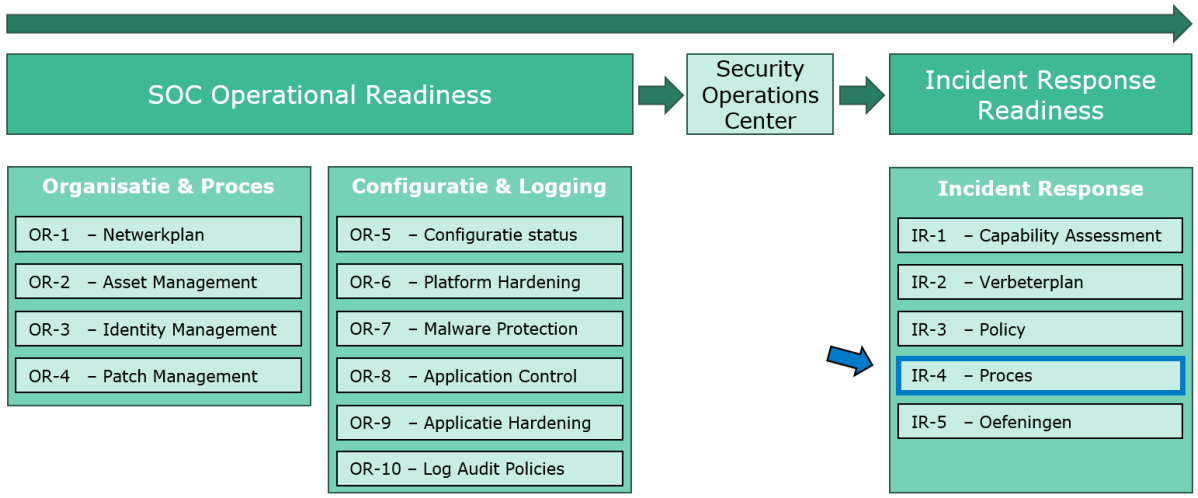
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de Incident Response **miniproducten**. De Incident Response Readiness miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze 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-minipoducten raamwerk.



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

De documenten onder IR-4 Proces bestaan uit:

- Procesmodel
  PDF document voorziet in het procesmodel voor Incident Response

- Procesimplementatie (**Dit document**)
  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 en de procesimplementatie.

3.1 Voorbereiding

Voordat je dit document gebruikt:

- Zorg dat je het kennisdocument 'Procesmodel (IR-4)' hebt doorgenomen en;
- 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.

Hoofdstuk 4 beschrijft een zestal stappen die gebruikt kunnen worden om het procesmodel voor incidentresponse, zoals beschreven in het 'Procesmodel (IR-4)', te implementeren.

3.3 Wat is het doel van dit document?

Dit document helpt je om binnen de context van informatiebeveiliging:

- Het incident- en responsemanagementproces via een gestructureerde aanpak te implementeren;
- Vaststellen van de juiste processen en tools;
- Het betrekken van de juiste mensen en rollen;
- Het trainen van teams;
- Het integreren van technologieën die bijdragen aan een efficiënte en gecoördineerde incidentresponse;
- te voldoen aan eisen vanuit de BIO en de NIS2-richtlijn.

3.4 Gebruik van dit document

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

- Als hulpmiddel om de processen die beschreven zijn in het kennisdocument 'Procesmodel (IR-4) te implementeren;
- Als ondersteuning bij de optimalisatie of uitbreiding van bestaande beveiligingsincident- & responseprocessen.

4 Implementatie

In dit document wordt de implementatie van het 'Procesmodel (IR-4)' beschreven. Hierbij worden acht verschillende stappen beschreven voor een succesvolle implementatie van het incident en response proces.

4.1 Inleiding

Een succesvolle implementatie van een incident- en responsemanagementproces vereist een gestructureerde aanpak die meerdere fasen doorloopt. Deze fasen omvatten niet alleen het vaststellen van de juiste processen en tools, maar ook het betrekken van de juiste mensen en rollen, het trainen van teams, en het integreren van technologieën die bijdragen aan een efficiënte en gecoördineerde incidentresponse. Het uiteindelijke doel is om zowel de organisatie als de verschillende rollen in staat te stellen om snel en adequaat te reageren op beveiligingsincidenten, hetgeen resulteert in een snellere hersteltijd en een verhoogde weerbaarheid tegen toekomstige incidenten.

4.2 Implementatie stappenplan

Hieronder worden acht stappen verder uitgewerkt van de implementatie van het incident en response procesmodel. Dit wordt gedaan aan de hand van een beschrijving, doel, acties en overwegingen.

Stap 1: Behoefte en doelstellingen

Beschrijving:
Deze stap richt zich op het analyseren van de huidige processen, tools en verantwoordelijkheden omtrent beveiligingsincidenten. Door de kloof tussen de huidige en gewenste situatie te identificeren, kunnen gerichte verbeteringen worden aangebracht.

Doel:
Het vaststellen van de huidige situatie en de gewenste uitkomsten voor het incident- en responseproces, zodat een duidelijk actieplan kan worden ontwikkeld.

Acties:

- Beoordeel de huidige situatie: Identificeer bestaande processen, tools en verantwoordelijkheden met betrekking tot het afhandelen van beveiligingsincidentbeheer. Onderzoek de bestaande technische infrastructuur, zoals monitoringtools, logs, incidentregistratie, en communicatieplatforms;

- Identificeer de gewenste situatie: Stel duidelijke doelen voor de implementatie, zoals het verkorten van de reactietijd bij incidenten, het verbeteren van de samenwerking tussen teams, of het verbeteren van de documentatie en rapportages;

- Identificeer de kloof: Vergelijk de huidige situatie met de gewenste situatie en zoek naar tekortkomingen. Breng de geïdentificeerde kloof in kaart en stel prioriteiten op basis van hun impact op de organisatie. Ontwikkel een actieplan om de benodigde verbeteringen door te voeren. Dit kan zowel korte termijn- als lange termijn maatregelen bevatten.

Overwegingen:

- Risicoanalyse: Voer een grondige risicoanalyse uit om de belangrijkste dreigingen en kwetsbaarheden te identificeren. Dit helpt bij het stellen van prioriteiten en het bepalen van de belangrijkste focusgebieden voor incidentresponse;
- Ontwikkel: Maak Kritieke Prestatie Indicators (KPI's) om de gewenste situatie meetbaar te maken.

Stap 2: Organisatie en rollen

Beschrijving:
Deze stap omvat het toewijzen van specifieke rollen aan medewerkers, waarbij de benodigde kwalificaties en verantwoordelijkheden voor elke rol duidelijk worden gedefinieerd.

Doel:
Het definiëren van de benodigde rollen en verantwoordelijkheden binnen de organisatie voor een effectief incident- en responseproces.

Acties:
Let op: Indien de benodigde rollen nog niet zijn ingevuld, kunnen deze tijdelijk worden toegewezen aan bestaande medewerkers. Voor de langere termijn kunnen nieuwe medewerkers worden aangetrokken.

Het is aanbevolen om de volgende rollen in te vullen:

- Security incident en response manager (SIRM): Deze dient een grondige kennis van incidentenbeheer, IT-beveiliging, en het oplossen van beveiligingsincidenten te hebben en het vermogen om multidisciplinaire teams aan te sturen.

  De SIRM moet nauw samenwerken met zowel de beveiligingsanalist als de Security incidentresponder om het incident van begin tot eind te beheren. De SIRM speelt ook een sleutelrol in de communicatie en (voortgangs)rapportage aan het management (zoals de CISO) en andere belangrijke belanghebbenden;

- Security analist: Heeft kennis van netwerken, IT-systemen, malware, forensisch onderzoek en beveiligingstechnieken. De analist is in staat om diepgaande analyses van incidenten uit te voeren om oorzaken en impact te identificeren.

  De security analist werkt hand-in-hand met de Security incidentresponder om de technische details van een incident te onderzoeken en de benodigde herstelmaatregelen vast te stellen. Deze biedt technische ondersteuning bij het vaststellen van de oorzaken en adviseren over de benodigde mitigatie;

- Security Incident Responder: Zeer ervaren met IT-systemen en netwerken, besturingssystemen, applicaties en beveiligingsprotocollen. Dit houdt in dat ze vertrouwd zijn met technieken zoals netwerksegmentatie, firewalls, intrusion detection/prevention systems (IDS/IPS), en encryptie. Daarnaast is kennis van malware-analyse, forensics en kwetsbaarheidsbeheer essentieel om effectief te kunnen reageren op incidenten zodat de herstelmaatregelen snel en efficiënt kunnen worden geïmplementeerd. De responder moet in staat zijn om zowel tijdelijke als permanente herstelmaatregelen te selecteren en te implementeren of hierop toezien.

  De Security incident responder werkt direct samen met de security analist voor technische ondersteuning en met de SIRM voor een goede coördinatie en documentatie van alle herstelmaatregelen. Deze zorgt ervoor dat alle systemen weer operationeel zijn op het gewenste niveau en dat het incident volledig wordt afgehandeld;

- Information Security Officer (ISO): Deze dient adequate kennis van gerelateerde wet- en regelgeving te hebben en kennis over frameworks waaronder de BIO en de NIS2. De ISO heeft ervaring met het ontwikkelen, implementeren en onderhouden van informatiebeveiligingsbeleid.

  De ISO speelt een belangrijke rol bij post-incident evaluaties. Deze werkt nauw samen met de CISO om de bredere strategie en compliance-vereisten te borgen en met de SIRM voor de analyse van incidenten en de implementatie van verbetermaatregelen;

- Chief Information Security Officer (CISO): Uitgebreide ervaring in informatiebeveiliging, strategisch leiderschap, risicobeheer en compliance. Vaardigheid in communicatie met het hoger management en bestuur.

  De CISO ontwikkelt en onderhoudt de strategische visie voor de informatiebeveiliging van de

organisatie en communiceert beveiligingsrisico's en incidenten aan het hoger management en het bestuur, en zorgt voor een adequate response.

Overwegingen:
- Huidige capaciteiten en rollen: Evalueer de huidige capaciteiten en rollen van de organisatie die incidenten detecteren en te beheren. Dit omvat de huidige tools, processen, en beschikbare medewerkers. Indien nodig, dienen er investeringen in nieuwe tools, trainingen en/of personele capaciteit te worden gepleegd;
- In de context van rolverdeling: In organisaties kan het uitdagend zijn om de bepaalde cybersecurity-rollen te vervullen, gezien de beperkte personeelsbezetting. Hoewel functies zoals Chief Information Security Officer (CISO) en Information Security Officer (ISO) doorgaans als afzonderlijke posities worden gezien, is het mogelijk dat één persoon beide rollen op zich neemt. Dit biedt de organisatie de kans om de benodigde expertise te centraliseren en tegelijkertijd de efficiency te verhogen.

Stap 3: procedures opstellen

Beschrijving:
In deze stap worden de processen hoe men voor een incidentresponse en specifieke responseplan voor verschillende dreigingscategorieën opstelt, evenals evaluatieprocedures voor verbeteringen.

Doel:
Het ontwikkelen van duidelijke procedures voor het afhandelen van beveiligingsincidenten, zodat een gestructureerde response kan worden gegarandeerd.

Actie:
- Ontwikkel een regulier beveiligingsincident response proces: Door eerst de specifieke behoeften, risico's en bedreigingen van de organisatie te analyseren en de belangrijkste assets te identificeren. Stel een incident response team samen met relevante medewerkers uit verschillende disciplines, zoals IT, beveiliging en juridische zaken. Stel het proces op met duidelijke onderdelen, inclusief detectie, beoordeling, reactie, herstel en evaluatie. Bepaalde onderdelen worden verder behandelt in de onderstaande stappen.

- Ontwikkel incident-specifieke responseplannen: Voor dreiging categorieën (malware-aanvallen, phising, data-inbreuken, etc) moeten responseplannen worden ontwikkeld, met duidelijk gedefinieerde doelen. Deze plannen moeten in lijn zijn met de RACI-matrix van het VSSR I&R IR4 beveiliginsincidentmanagement en –response proces om de impact van incidenten te minimaliseren.

- Responseplan evaluatie: Zorg voor een standaard jaarlijkse review aan de ontwikkelde responseplannen en actualiseer deze ad hoc wanneer evaluaties van incidenten hier aanleiding toe geven.

Overwegingen:
- Informatie inventarisatie: Zorg voor een goede inventarisatie van beschikbare informatie onder meer bij bronnen als het NCSC, de eigen IT- beheerorganisatie of NIST.
- Meldingen: Zorg dat in de verschillende procedures ook duidelijk is welke communicatieverplichtingen er zijn (b.v. meldplicht aan in- en externe stakeholders). Hierbij kan gekeken worden naar het escalatieplan van stap 7.
- Tijdfactor: Zorg dat verplichtingen in de tijd duidelijk zijn, binnen hoeveel tijd melden, communiceren, escaleren, etc. Hierbij kan gekeken worden naar het escalatieplan van stap 7.

Stap 4: Het classificeren en prioriteren

Beschrijving:
Deze stap omvat het ontwikkelen van een classificatiesysteem voor verschillende typen incidenten en het opstellen van een impact- en urgentietabel om prioriteiten te bepalen.

Doel:
Het systematisch classificeren en prioriteren van incidenten om efficiënt en effectief te reageren op beveiligingsincidenten.

Actie:

- Incident classificatie: Het ontwikkelen van een classificatie voor verschillende type incidenten (bijv. malware, datalek, netwerkincident);

- Impact en urgentie tabel: Maak een tabel om de impact en urgentie vast te stellen (bijvoorbeeld zeer hoog, laag, zeer laag). Deze tabel stelt de organisatie in staat om op consistente wijze een keuze te maken. Op basis waarvan een prioriteit (1, 2, 3, of 4) kan worden bepaald.

  Bijvoorbeeld:
  - Prio 1: Er is sprake van Prio-1 als één of meerdere van de volgende situaties zich voordoet:
    - Bedrijfsvoering is ernstig verstoort of bedreigd.
    - De organisatie kan niet aan haar wettelijke taken/verplichtingen voldoen.
    - Er is (potentieel) media-aandacht.
    - Grote impact op burgers/bedrijven.
    - (kans op) politieke aandacht.
    - grote kans dat het incident zich verder verspreid en meer schade veroorzaakt.

  - Prio 2: Er is sprake van Prio-2 indien één of meerdere van de volgende situaties zich voordoet:
    - Bedrijfsvoering wordt gehinderd of bedreigd maar de organisatie kan wel aan haar wettelijke taken/verplichtingen voldoen.
    - Merkbare impact voor burgers/bedrijven.
    - Risico dat het incident zich verder uitbreidt.
    - Er is een beperkte vorm van media-aandacht.

  - Prio 3: Er is sprake van Prio-3 indien in tenminste alle onderstaande situaties van toepassing zijn:
    - De hinder van het incident is beperkt tot de interne bedrijfsvoering en raakt geen burgers of bedrijven en;
    - de organisatie kan aan haar wettelijke taken en verplichtingen voldoen.
    - Er zijn geen aanwijzingen dat het incident zich noemenswaardig uitbreidt.

  - Prio 4: Er is sprake van een Prio-4 incident indien tenminste alle onderstaande situaties van toepassing zijn:
    - De bedrijfsvoering ondervindt weinig tot geen hinder van het incident en;
    - uitsluitend de interne organisatie wordt geraakt.
    - Het incident leidt niet tot schade voor de organisatie of derden en de organisatie kan aan haar wettelijke verplichtingen en taken voldoen.
    - Er is geen risico dat het incident zich verder uitbreidt.

Overwegingen:

- Flexibiliteit: Afhankelijk van nieuw verkregen inzichten dient de prioriteit en/of classificatie van het individuele incident opnieuw te worden vastgesteld.

Stap 5: Tools en infrastructuur

Beschrijving:
In deze stap wordt uitgelegd hoe men de functionele en technische vereisten voor incidentbeheer-tools vast kan stellen.

Doel:
Het identificeren en implementeren van de juiste tools en infrastructuur die nodig zijn voor effectief incidentbeheer.

Acties:
- Functionele vereisten: Bepaal en documenteer de functionele vereisten voor de incidentbeheertools. Wat de benodigde functionele vereisten zijn, kan bijvoorbeeld in kaart worden gebracht door middel van een workshop met belanghebbende. Men kan dan de vereisten identificeren, zoals incidentregistratie, prioritering, rapportage en integratiemogelijkheden;

- Implementeer functionaliteit: Implementeer de vereiste functionaliteit in incidentbeheertools zoals IT-servicemanagement systemen (ITSM-systemen) zodanig dat deze aansluiten bij de specifieke behoeften van de organisatie. Zorg ervoor dat de tools goed integreren met andere IT-systemen, zoals monitoringtools, antivirussoftware, en logmanagementsystemen. Denk hierbij ook aan koppeling met systemen van ketenpartners en toeleveranciers;

- Technische vereisten: Identificeer de specifieke technische vereisten voor de tools (bijv. compatibiliteit met bestaande systemen, mogelijkheden voor realtime monitoring, enz.) die nodig zijn om incidenten effectief te beheren.

Overwegingen:
- Gebruiksvriendelijkheid: De gebruikte tools moeten gebruikersvriendelijk zijn. Dit bevordert snelle adoptie en efficiënt gebruik bij incidenten afhandeling. Training en documentatie moeten beschikbaar zijn om het gebruiksgemak te ondersteunen;
- Informatievoorziening: Zorg ervoor dat alle betrokkenen, zoals de SIRM, security analisten en security incident responders, up-to-date geïnformeerd worden over incidenten met toegang tot het incidentbeheersysteem;
- Rapportage en analyses: Zorg dat er op een systematische manier rapportage en analyses worden gemaakt om achteraf evaluaties en lessons learned te faciliteren. Dit zorgt dat er continue verbetering kan plaatsvinden binnen het gebruik van de tools en infrastructuur.

Stap 6: Trainingen en opleiding

Beschrijving:
Deze stap betreft het opstellen van een opleidingsprogramma voor medewerkers en het uitvoeren van oefeningen om de samenwerking te verbeteren.

Doel:
Het waarborgen van de juiste kennis en vaardigheden binnen de organisatie om effectief te reageren op beveiligingsincidenten.

Acties:
- Ontwikkel: Stel een programma op voor de training van alle medewerkers die betrokken zijn bij het beveiligingsincidentmanagement en –response. Dit programma moet een groeipad van competenties omvatten, waarbij de integraliteit van de training wordt gewaarborgd. Het opleidingsniveau van verschillende rollen moet op elkaar aansluiten om een effectieve samenwerking en kennisoverdracht te bevorderen. Zorg ervoor dat het programma zowel basis- als gevorderde trainingen biedt, afgestemd op de specifieke verantwoordelijkheden en taken van de medewerkers. Dit kan onder meer inhouden dat er modules worden ontwikkeld voor verschillende functieniveaus of rollen, zodat medewerkers op elk niveau of bij elke rol de juiste kennis en vaardigheden opdoen om adequaat te reageren op beveiligingsincidenten;

- Oefeningen uitvoeren: Voer regelmatig oefeningen of 'tabletop exercises' uit, waarbij beveiligingsincident scenario's worden nagebootst die de organisatie kunnen treffen. Dit kan helpen om de reactietijd te versnellen en de efficiëntie van het proces door het team te verbeteren.

Overwegingen:
- Training: Het is geen eenmalige activiteit, maar een continu proces. Nieuwe medewerkers moeten snel worden ingewerkt, en bestaande medewerkers moeten regelmatig op de hoogte worden gebracht van nieuwe tools, dreigingen en trends in incidentresponse.

Stap 7: Communicatie en escalatieprocedures

Beschrijving:
In deze stap worden de procedures voor de escalatie van incidenten en de communicatie eromheen gedefinieerd, zodat de betrokken partijen tijdig en correct wordt geïnformeerd.

Doel:
Het opzetten van duidelijke communicatie- en escalatieprocedures om ervoor te zorgen dat incidenten effectief worden gemeld en beheerd.

Acties:
- Escalatieprocedure: Definieer wanneer, hoe en door wie incidenten moeten worden geëscaleerd. Wanneer bijvoorbeeld de afhandeling van een incident de operationele capaciteit van een team overschrijdt of de reputatie van de organisatie direct in gevaar brengt, moet onmiddellijk hoger management worden ingeschakeld of worden geëscaleerd naar het crisismanagement proces.

  Zet een escalatieplan op zodat bekend is wie het mandaat heeft tot escalatie bij welke impact en urgentie;

- Communicatieprocedure: Stel een communicatieprocedure op die definieert wanneer, hoe en door wie communicatie over incidenten moet plaatsvinden. Bepaal welke informatie aan medewerkers, klanten en leveranciers moet worden verstrekt, afhankelijk van de ernst van het incident. Zorg voor duidelijke richtlijnen om interne en externe communicatie effectief te coördineren, zodat iedereen tijdig en juist geïnformeerd is.

  Zie Bijlage I *Voorbeeld communicatieplan.*

Overwegingen:
- Betrek de belanghebbenden: Communicatie moet niet alleen intern, maar ook extern worden gecoördineerd in de gehele IT-keten dus ook naar klanten en leveranciers, afhankelijk van de ernst van het incident. Breng in kaart welke incidenten tot politieke aandacht kunnen leiden. Stem waar nodig communicatieprocedures af met communicatieafdelingen en persvoorlichting;
- Inschakelen van forensische expertise: Overweeg om forensische expertise in te schakelen als onderdeel van de escalatieprocedure, vooral bij ernstige incidenten. Te laat inschakelen kan leiden tot verlies van bewijsmateriaal of het onbruikbaar maken ervan. Zorg ervoor dat er duidelijke richtlijnen zijn voor het tijdig betrekken van forensische experts om de effectiviteit van het onderzoek te waarborgen.

Stap 8: Monitoren en continue verbetering

Beschrijving:
Deze stap omvat het uitvoeren van evaluaties na incidenten en het opstellen van verbeterplannen op basis van de bevindingen.

Doel:
Het evalueren en verbeteren van het incidentmanagementproces op basis van ervaringen en gegevens uit eerdere incidenten.

Acties:

- Evaluatie en verbeterplan: Voer na een prioriteit 1 of 2 incident een evaluatie uit. Analyseer wat goed ging en welke verbeteringen nodig zijn in het ontwerp of de uitvoering van de processen. Werk een verbeterplan uit dat is gebaseerd op de bevindingen van deze evaluaties.

- Beoordeling: Evalueer KPI's op om de effectiviteit van het beveiligingsincidentmanagement en –response proces te monitoren. Dit kan bijvoorbeeld de gewenste gemiddelde of maximale reactietijd zijn vanaf binnenkomst van de melding, de tijd tot volledige herstel van de IT-dienstverlening, of de frequentie van incidenten per maand zijn.

Overwegingen:

- Effectiviteit beoordelen: Gebruik registraties en de gekozen KPI's om de effectiviteit van het beveiliginsincidentmanagement en –response proces te beoordelen. Hierdoor kan de organisatie objectief bepalen waar verbeteringen nodig zijn in het ontwerp of de uitvoering van het proces en gericht verbeteracties ondernemen.
- Flexibiliteit waarborgen: Aangezien dreigingen voortdurend veranderen, moet de organisatie zodanig flexibel zijn dat het incidentmanagement en –responseproces met ondersteunende tooling voldoende snel aanpassingen kan doorvoeren om nieuwe dreigingen aan te pakken. Dit kan bijvoorbeeld door stap 4 als een onafhankelijk proces te behandelen en zo de urgentie en impact flexibel te bepalen.
- IT Service management: Richt het systeem zodanig in dat bij de registratie van prioriteit-1 en prioriteit-2 incidenten, het servicemanagementsysteem - bij voorkeur automatisch - een ticket voor incidentevaluatie aanmaakt.

  Deze automatisering voorkomt dat evaluaties vergeten worden en zorgt ervoor dat deze op een gestructureerde manier worden vastgelegd. Hierdoor kan de evaluatie efficiënter en effectiever worden uitgevoerd, wat de kwaliteit van de incidentafhandeling ten goede komt.

Bijlage I Voorbeeld communicatieplan

	Beschrijving – Security Incident Management	Detectie	Reactie	Reminder	Algemene procedures		IT-beheer organisatie
Priority 1 (Prio 1)	Wanneer zich één of meerdere kritieke situaties voordoen. Dit gebeurt wanneer de bedrijfsvoering ernstig verstoord of bedreigd is, wat kan leiden tot chaos en inefficiëntie binnen de organisatie. Daarnaast kan het zijn dat de organisatie niet in staat is om aan haar wettelijke taken en verplichtingen te voldoen, wat ernstige consequenties kan hebben. Ook als er een grote impact op burgers of bedrijven is, wordt dit als een reden voor Prio-1 beschouwd, net als de kans op politieke aandacht die kan ontstaan. Tot slot is er het risico dat het incident zich verder verspreidt en meer schade veroorzaakt, wat de urgentie om snel en effectief te reageren alleen maar vergroot.	15 min	30 min	1 uur	Informeer alle SOC's zo snel mogelijk per telefoon Stuur een e-mail/ticket naar alle SOC's Registreer het ticket in je eigen ticketsysteem en rapporteer in de maandelijkse operationele rapporten	Contact details	E-mail (stuur alstublieft naar onderstaande): - Voorbeeld@min.nl
						Procedure	Email + phone
Priority 2 (Prio 2)	- Een incident wordt geclassificeerd als Prio-2 wanneer de bedrijfsvoering gehinderd of bedreigd wordt, maar de organisatie nog steeds aan haar wettelijke taken kan voldoen. - Er is een merkbare impact voor burgers of bedrijven, en er bestaat risico dat het incident zich verder uitbreidt. Ook kan er sprake zijn van beperkte media-aandacht, wat de situatie aandachtwaardig maakt.	30 min	1 uur		- Informeerde security incidentresponder zo snel mogelijk per telefoon - Stuur een e-mail/ticket naar alle SOC's - Registreer het ticket in je eigen ticketsysteem en rapporteer in de maandelijkse operationele rapporten.	Contact details	E-mail (stuur alstublieft naar onderstaande): - Voorbeeld@min.nl
						Procedure	Email + phone

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