TLP:GREEN

IR-2 VERBETERPLAN

Incident Response - Incident Response Readiness

Best Practice versie 1.2

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	11-06-2025	Initiële versie
V1.1	16-06-2026	Foutcorrecties hoofdstuknummering en verwijzingen
V1.2	29-6-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Incident Response – Capability Assessment	Zie "IR-1, Incident Response – Capability Assessment (Excel) & Toelichting (pdf)" onder Incident Response Readiness
Incident Response Readiness miniproducten	Zie Incident Response Readiness op het VSSR-portaal
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.

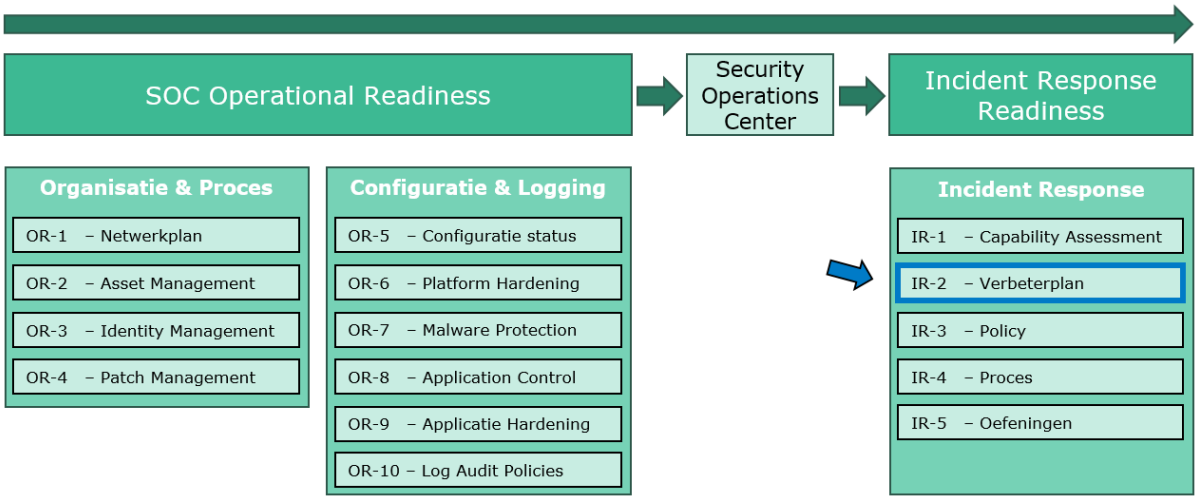
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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-2 Verbeterplan bestaan uit:

- Verbeterplan (**Dit document**)
  PDF document voorziet in implementatieplannen om naar een volgend capability niveau toe te werken.

3 Leeswijzer

Dit document is een (model) verbeterplan voor het versterken van het incident response-vermogen van jouw organisatie. Het is bedoeld om concrete handvatten te bieden voor het doorvoeren van verbeteringen op basis van de uitkomsten van het IR1 Capability Assessment.

3.1 Voorbereiding

Voordat je dit document gebruikt:

- Zorg dat het IR1 – Capability Assessment is uitgevoerd.
- Zorg dat je bekend bent met de structuur van het assessment: acht thema's en vier niveaus zoals in IR1 Assessment toelichting beschreven.

Realiseer je dat dit document is gebaseerd op dezelfde structuur als het assessment. In 'IR1-Assessment toelichting' is de structuur beschreven.

3.2 Structuur van dit verbeterplan

Dit document is opgebouwd in vier hoofddelen:

- Niveau 0: Wat moet minimaal op orde zijn;
- Van Niveau 0 naar Niveau 1: Begin naar basis;
- Van Niveau 1 naar Niveau 2: Basis naar uitgebreid;
- Van Niveau 2 naar Niveau 3: Uitgebreid naar risicogestuurd.

Binnen elk van deze delen komen telkens dezelfde acht thema's terug:

1. Beleid
2. Proces
3. Rollen
4. Meldbronnen
5. Responseplannen
6. Responsebereik
7. Testen & Oefeningen
8. Evaluatie

Voordat deze verbeterstappen worden uitgewerkt, bevat hoofdstuk 5 een toelichting op de risico's die kunnen ontstaan bij onvoldoende invulling van deze thema's. Dit kan helpen om inzicht te krijgen in de kwetsbaarheden die zich kunnen voordoen als bepaalde thema's ontbreken of onvoldoende zijn ingericht. Dit biedt belangrijke context voor het prioriteren van verbeteracties.

3.3 Gebruik van dit document

Je hoeft dit document niet van begin tot eind te lezen. Gebruik het doelgericht op basis van de uitkomsten van het IR1 – Capability Assessment.

Volg de onderstaande stappen voor een effectief resultaat:

- Voer het assessment uit (zie document IR1 – Capability Assessment);
- Bepaal per thema het huidige niveau van jouw organisatie;
- Kies één of meerdere thema's waarop je een verbetering wilt realiseren;
- Ga naar het hoofdstuk van het bijbehorende niveau (bijv. "Niveau 1 naar Niveau 2");
- Zoek binnen dat hoofdstuk het relevante thema (bijv. "Processen" of "Responseplannen");
- Voer de beschreven acties uit om het volgende volwassenheidsniveau te bereiken.

Elk hoofdstuk bevat concrete, uitvoerbare acties per thema. Het is niet nodig om eerdere niveaus door te nemen, tenzij je een volledig overzicht zoekt.

Gebruik dit (model) verbeterplan als basis voor:
- Het opstellen van verbetertrajecten of roadmaps;
- Het plannen van werkpakketten;
- Sprintmatige uitvoering binnen je organisatie.

Het verbeterplan is flexibel inzetbaar, afhankelijk van de prioriteiten, risico-inschatting en het verandervermogen van jouw organisatie. Zorg voor compacte en overzichtelijke werkpakketten die binnen een redelijke termijn, maximaal enkele weken, gerealiseerd kunnen worden.

4 Inleiding

Incidentmanagement is een belangrijk onderdeel van de informatiebeveiligingsstrategie van een organisatie. Het stelt de organisatie in staat om beveiligingsincidenten tijdig te detecteren, te beoordelen en op te lossen, terwijl de impact op de bedrijfsvoering wordt geminimaliseerd. De capability levels uit het "Incident Response – Capability Assessment" (0 tot 3) bieden een progressiemodel, zodat organisaties vanuit een situatie met ad-hoc processen naar een risico geoptimaliseerd incidentmanagement kunnen groeien. Waar het Capability Assessment inzicht verschaft in het huidige niveau, biedt dit implementatieplan de handvatten om de groei tussen het huidige en het gewenste niveau te realiseren.

Verschillende kaders en richtlijnen zoals de Baseline Informatiebeveiliging Overheid (BIO), het NIST Cybersecurity Framework (CSF) en de NIS2-richtlijn helpen bij het organiseren van informatiebeveiliging. Hoewel elk van deze raamwerken zijn eigen specifieke vereisten en focusgebieden heeft, delen ze een gemeenschappelijk doel: het minimaliseren van de impact van beveiligingsincidenten en het versterken van de weerbaarheid.

5 Uitkomst Capability Assessment

Het resultaat van het "Incident Response – Capability Assessment" geeft een statusindicatie van de organisatie en een overzicht waarop de organisatie moet focussen om beveiligingsincident- & responsemanagement verder te verbeteren.

Onderstaande matrix toont de Capability niveaus en status per onderwerp.

Beveiligingsincident- & responsemanagement assessment matrix								
Capability Niveau	**Beleid**	**Proces**	**Rollen**	**Meld-bronnen**	**Response-plannen**	**Response-bereik**	**Testen & Oefeningen**	**Evaluatie**
Niveau 0 (Begin)	Nee	Generiek	Generiek	Gebruikers	Nee	IT-systemen	Nee / Nee	Nee
Niveau 1 (Basis)	Ad hoc	Beveiligings-incident	Beveiligings-incident	Basis monitoring	1 generiek	IT-systemen met business	Ja / Nee	Na crisis
Niveau 2 (Uitgebreid)	Instrumenteel	Beveiligings-response	Response	SOC	3 basis plannen	IT-systemen, diensten en business	Ja / Tabletop	Bij prio 1 incidenten
Niveau 3 (Risico-Geoptima-liseerd)	Structu-reel	Geïntegreerd	Specialisten	Cyber Defense Center	Op maat	Informatie keten	ART of TIBER	Altijd

Tabel 1 Capability-niveaus matrix

5.1 Risicobehandeling van de criteria

In dit document ligt de focus op het inrichten van de volgende onderdelen met betrekking tot incidentresponse: beleid, proces, rollen, meldbronnen, responseplannen, responsebereiktesten & oefeningen en evaluatie (zie Tabel 1). Bij onvoldoende invulling van deze criteria kunnen

verschillende risico's ontstaan die de effectiviteit van beveiligingsincident- & responsemanagement beïnvloeden. Hieronder wordt een korte toelichting gegeven op de risico's die kunnen ontstaan bij onvoldoende aandacht voor deze criteria.

5.1.1 Beleid

Voor incidentresponse is het noodzakelijk dat er beleid is dat kaders, verantwoordelijkheden en doelstellingen voor het reageren op beveiligingsincidenten beschrijft. Het ontbreken of onvoldoende invulling van een incidentresponsebeleid kan ervoor zorgen dat het herstel van beveiligingsincidenten niet goed aansluit bij de doelstellingen van de organisatie. Zonder duidelijk beleid kunnen de juiste keuzes en prioriteiten in het beveiligingsincidenten-proces niet altijd goed of tijdig worden gemaakt, wat kan leiden tot ongewenst ernstige verstoringen in bedrijfsprocessen of kwetsbaarheden in bedrijfskritische systemen. Dit kan de bedrijfscontinuïteit beïnvloeden. Om dit risico te verminderen, is het van belang om een volledig incidentresponsebeleid te ontwikkelen dat duidelijk de stappen, verantwoordelijkheden en prioriteiten vastlegt. Dit beleid moet regelmatig worden herzien en aangepast aan de veranderende dreigingen en bedrijfs- en IT-doelstellingen.

5.1.2 Proces

Duidelijke procesbeschrijvingen zijn essentieel voor het goed functioneren van incident response. Onduidelijke of onvolledige processen kunnen de reactietijd verhogen en het incidentresponseproces vertragen. Daarnaast bestaat er ook een risico dat incidenten verkeerd worden geprioriteerd, wat (kritische) bedrijfsprocessen ongewenst kan verstoren of vertragingen kan veroorzaken in het uitvoeren van noodzakelijk mitigerende maatregelen. Om dit risico te beperken, is het belangrijk om gestandaardiseerde processen en procedures voor incidentresponse te implementeren. Deze processen moeten regelmatig worden herzien en getest om ervoor te zorgen dat ze effectief en efficiënt blijven, zelfs bij beveiligingsincidenten met grotere impact.

5.1.3 Rollen

Voor een effectief incidentresponse is het noodzakelijk dat alle betrokkenen weten wat hun rol is en welke taken ze hebben. Onvoldoende duidelijkheid over de rollen en verantwoordelijkheden kan leiden tot onduidelijkheid over de besluitvorming van mitigerende maatregelen waardoor het risico op onnodige verstoringen en/of kwetsbaarheden in bedrijfsprocessen onnodig wordt vergroot. Om dit risico te reduceren, is het noodzakelijk om rollen en verantwoordelijkheden helder te omschrijven en duidelijk toe te wijzen. Dit moet worden vastgelegd in een gedetailleerd overzicht met welke rol welke acties onderneemt tijdens beveiligingsincidenten, zodat iedereen snel en efficiënt kan handelen.

5.1.4 Meldbronnen

Meldbronnen zijn alle objecten en voorzieningen die signalen aan monitoringsystemen geven waarmee het mogelijk is om onregelmatigheden in ICT-systemen te detecteren. Het gebrek aan monitoring van meldbronnen kan ervoor zorgen dat meldingen niet tijdig worden opgemerkt, wat leidt tot vertraging in de reactie op gedetecteerde beveiligingsincidenten. Wanneer meldingen uit verschillende bronnen niet juist, tijdig en volledig worden verzameld, kunnen belangrijke signalen worden gemist. Om dit risico te verlagen, moet er een centraal meldsysteem worden opgezet dat meldingen van verschillende bronnen samenbrengt en overzichtelijk weergeeft ("single pane of glass"-monitoring). Hiermee kunnen meldingen snel en effectief worden beheerd en geanalyseerd.

5.1.5 Responseplannen

Een responseplan beschrijft hoe een organisatie snel en effectief kan reageren op cyberaanvallen of datalekken. Onvolledige of verouderde responseplannen leiden tot fouten en vertragingen bij de afhandeling van beveiligingsincidenten. Wanneer plannen niet goed zijn afgestemd op actuele dreigingen, kunnen organisaties niet adequaat reageren, wat de impact van beveiligingsincidenten vergroot. Om dit risico te verminderen, moeten responseplannen regelmatig worden gecontroleerd en bijgewerkt. Door ervoor te zorgen dat de plannen altijd up-to-date zijn, wordt de organisatie beter voorbereid op de afhandeling van beveiligingsincidenten.

5.1.6 Responsebereik

Het responsebereik heeft betrekking op de omvang van systemen, processen en data die betrokken zijn bij incidentresponse. Wanneer niet alle systemen en gegevens worden meegenomen in de response, kan de totale impact van een beveiligingsincident onnodig groter worden. Dit komt vaak voor wanneer er geen volledig en juist overzicht is van alle kritieke systemen en applicaties die getroffen kunnen worden. Om dit risico te reduceren, is het noodzakelijk om het responseplan af te stemmen met eigenaren van alle bedrijf kritische systemen, applicaties en gebruikers. Dit zorgt ervoor dat geen enkel belangrijk systeem van de organisatie onterecht buiten de response valt.

5.1.7 Testen & Oefeningen

Het testen richt zich op het incidentresponseplan zelf en is bedoeld om te controleren of het plan werkt zoals beoogd en om eventuele fouten in het incidentresponseplan op te sporen. Het oefenen richt zich op medewerkers en is bedoeld om ervaring op te bouwen met het gebruik van deze plannen. Het onvoldoende testen van en oefenen met incidentresponseplannen kan ervoor zorgen dat teams niet goed zijn voorbereid op daadwerkelijke incidenten. Het ontbreken van oefeningen kan leiden tot een situatie waarin medewerkers onvoldoende vaardig zijn om snel en effectief te reageren wanneer een beveiligingsincident wordt gemeld. Om dit risico te verminderen, moeten er regelmatig tabletop oefeningen en simulaties van beveiligingsincidenten worden gehouden. Deze oefeningen helpen niet alleen om de inhoud van de plannen te beoordelen, maar ook om teams in de uitvoering te laten oefenen waardoor hun reactiecapaciteiten worden verbeterd.

5.1.8 Evaluatie

Het is belangrijk om beveiligingsincidenten te evalueren. Het ontbreken van een gedegen evaluatie na elk prio-1 en -2 incident brengt het risico met zich mee dat fouten zich in de toekomst herhalen, en dat processen niet verbeterd worden. Evaluaties zijn belangrijk om van beveiligingsincidenten te leren en de effectiviteit van de response te verbeteren. Na elk beveiligingsincident moet er een gedetailleerde evaluatie plaatsvinden, waarbij verbeterpunten worden vastgesteld, gedocumenteerd en verwerkt in het incidentresponseplan, zodat de organisatie beter is voorbereid op toekomstige beveiligingsincidenten.

6 Implementatieplan

De tijd die nodig is om een hoger capability-niveau te bereiken en een effectiever beveiligingsincident & responseproces in te richten, is sterk afhankelijk van het verandervermogen van de organisatie. Factoren zoals beschikbare middelen, betrokkenheid van het management, bestaande processen en de adoptiesnelheid van nieuwe technologieën spelen hierbij een belangrijke rol. Effectieve implementatie is afhankelijk van specifieke omstandigheden binnen de organisatie en kunnen variëren door interne en externe factoren.

In dit hoofdstuk worden per niveau doelstellingen en generieke uitdagingen geformuleerd die organisaties helpen bij het verbeteren van hun incident- & responsemanagement. Deze uitdagingen bieden inzicht in de gebieden waar verbetering mogelijk is. Daarnaast zijn er praktische actiepunten gedefinieerd die organisaties kunnen uitvoeren om de vereisten van elk niveau te vervullen. Deze gestructureerde aanpak biedt een startpunt voor het ontwikkelen van een incidentresponsestrategie en helpt organisaties de noodzakelijke processen en maatregelen te implementeren.

6.1 Niveau 0

Doel: Begin met het integreren van digitale weerbaarheid bij het senior management en het implementeren van duidelijke procedures voor het melden en afhandelen van beveiligingsincidenten.
In de volgende paragrafen is beschreven wat er moet worden geïmplementeerd om niveau 0 te bereiken.

6.1.1 Beleid

Neem met betrekking tot het beleid de volgende acties:

- Bepaal wat als beveiligingsincident wordt beschouwd binnen de organisatie en zorg ervoor dat deze definitie wordt gedocumenteerd in een beleidsdocument;

- Neem in het beleid concrete kaders op met betrekking tot het classificeren van incidenten. Hierbij moet gekeken worden naar het type incident dat kan voorkomen en de impact/urgentie ervan. Leg deze afspraken vast in een beleidsdocument, zodat voor iedereen duidelijk is welke classificatie aan een incident moet worden toegekend. Bijvoorbeeld prioriteit 1 bij een ransomware aanval;

- Voeg een sectie toe in het beleidsdocument die de verantwoordelijkheden van de verschillende teams beschrijft bij het omgaan met beveiligingsincidenten. Specificeer welke teams verantwoordelijk zijn voor: Het oplossen van incidenten, communicatie met interne en externe belanghebbenden, management van het incident en het coördineren van reacties (bijvoorbeeld crisismanagementteam);

- Zorg ervoor dat de bovenstaande acties zijn geïntegreerd in hetzelfde beleidsdocument en dat hun uitvoering plaatsvindt in overleg en met goedkeuring van het senior management.

6.1.2 Proces

Neem met betrekking tot het proces de volgende acties:

- Zorg dat de organisatie over een servicedesk beschikt die in staat is om beveiligingsincidenten aan te nemen, te registeren en de afhandeling aan te sturen.

- Zorg dat de servicedesk over servicemanagement-tooling beschikt dat de mogelijkheid biedt om:
  - Een incident moet ook te markeren zijn als als beveiligingsincident. Dit maakt het mogelijk om te filteren op beveiligingsincidenten en analyses uit te voeren;
  - Verschillende prioriteiten aan beveiligingsincidenten toe te kennen. Tevens moet er een werkproces c.q. werkinstructie zijn waarmee de servicedesk op consistente wijze een prioriteit aan beveiligingsincidenten kan toekennen;

  - Rapportages over beveiligingsincidenten te genereren.
    De rapportages bevatten minimaal:
    - Het aantal beveiligingsincidenten die in de rapportageperiode zijn gemeld;
    - Het aantal beveiligingsincidenten dat in de rapportageperiode zijn afgehandeld;
    - De prioriteit die aan deze beveiligingsincidenten zijn toegekend;
    - Doorlooptijden van deze beveiligingsincidenten;
    - De maatregel die genomen is om het beveiligingsincident op te lossen;
    - Het aantal openstaande beveiligingsincidenten.

  - Rapporteren over incidenten & beveiligingsincidenten. Dit is van belang om een scherp zicht te houden op de afhandeling van beveiligingsincidenten. en moet voorkomen dat beveiligingsincidenten ondersneeuwen door reguliere incidenten waardoor het zicht vertroebelt;
  - De voortgang van incidentherstel geautomatiseerd bewaken en richt bijbehorende werkprocessen zodanig in dat er gerappelleerd en/of geëscaleerd wordt bij traag of uitblijvend incidentherstel;
- Zorg dat de servicedesk toegang heeft tot de contactinformatie van alle belanghebbenden om deze te informeren bij beveiligingsincidenten. De servicedesk is op de hoogte van de wijze waarop deze belanghebbenden geïnformeerd moeten worden (telefonisch, mail, webportal, anders). Het gaat hier niet alleen om technische contactpersonen (oplosgroepen), maar ook om informatie-eigenaren, lijnmanagers en beveiligingsfunctionarissen;

- Zorg dat er is een proces is ingericht om aan de wettelijke meldplichten bij formele instanties zoals het CSIRT en Autoriteit Persoonsgegevens te voldoen. Houd bij het inrichten van een dergelijke proces rekening met de bevoegdheden van medewerkers.
  - Welke functionaris is bevoegd om de melding bij de formele instantie te doen?
  - Denk ook aan zaken als binnen hoeveel tijd en op welke wijze de betrokken functionarissen worden geïnformeerd.
- Zorg ervoor dat de standaard tooling voor het melden en afhandelen van IT-incidenten ook specifieke afhandelingsprocedures bevat voor beveiligingsincidenten;
- Documenteer de communicatie over kwetsbaarheden en beveiligingsincidenten om een duidelijk overzicht te hebben van de acties door betrokken partijen in de keten zoals het CSIRT, de Informatiebeveiligingsambtenaar, de CISO, IT-management en IT-dienstverleners.

6.1.3 Rollen

Neem met betrekking tot de rollen de volgende acties:

- Zorg ervoor dat er binnen de organisatie een Incidentresponse-manager is aangesteld, die verantwoordelijk is voor:
  - Begeleiden van incidenten en sturen op basis van aan het incident toegekende prioriteit;
  - Uitvoeren van evaluaties na incidenten om verbeteringen aan te brengen;
  - Op basis van aan het incident toegekende prioriteit escaleren naar de derde lijn;
  - Coördineren van communicatie en rapportage over incidenten aan het management en relevante stakeholders.
- Zorg ervoor dat er binnen de organisatie een Functionaris Gegevensbescherming is aangesteld, die verantwoordelijk is voor:
  - Toezicht houden op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en andere relevante privacywetgeving;
  - Adviseren van de organisatie over privacykwesties en gegevensbescherming;
  - Vraagbaak voor medewerkers met betrekking tot gegevensbeschermingskwesties;
  - Uitvoeren van privacy impact analyse en het rapporteren van bevindingen aan het management.
- Zorg ervoor dat er een Informatiebeveiligingsbeambte is aangesteld binnen de organisatie, die verantwoordelijk is voor:
  - Ontwikkelen, implementeren en onderhouden van het informatiebeveiligingsbeleid;

- Uitvoeren van risicoanalyses en audits om de effectiviteit van het beveiligingsbeleid te waarborgen;
- Rapporteren aan het management over de status van informatiebeveiliging en potentiële risico's voor de organisatie.

6.1.4 Meldbronnen

Neem met betrekking tot de meldbronnen de volgende acties:

- Zorg voor de aanwezigheid van servicemanagement-tooling en servicedesk waar beveiligingsmeldingen kunnen worden ontvangen. Maak standaardtemplates die ingevuld kunnen worden door werknemers wanneer er een melding wordt gemaakt;
- Maak een proces voor externe partijen om meldingen te doen bij de servicedesk of een ticketingsysteem. Stel indien mogelijk in overleg met interne en/of externe partijen een template op dat ingevuld moet worden bij een melding;
- Zorg ervoor dat flowcharts aanwezig zijn om de processtromen te verduidelijken bij het binnenkomen van nieuwe incidenten, zowel voor interne als externe meldingen;
- Zorg ervoor dat elk incident in het incidentbeheersysteem goed wordt gedocumenteerd met relevante details, zoals een uniek incidentnummer voor identificatie, de datum en tijd van melding, de betrokken personen, primaire contactpersonen, een beschrijving van het incident, de oorzaak en impact, de genomen acties om het op te lossen, en de datum en tijd waarop het incident is gesloten. Voeg ook eventuele bijlagen of bewijsstukken toe, zoals screenshots of logbestanden, om de documentatie te verduidelijken en toekomstige analyses te vergemakkelijken;
- Formuleer samen met relevante stakeholders een duidelijke procedure voor de routering van binnenkomende incidenten, zodat deze altijd bij de juiste oplosgroep terechtkomen. Dit houdt in dat je vastlegt wie verantwoordelijk is voor de ontvangst van incidentmeldingen en hoe deze meldingen beoordeeld en geprioriteerd moeten worden. Zorg ervoor dat incidenten met hoge prioriteit (prio 1) direct worden doorgestuurd naar de Incident Response Manager. Documenteer deze procedure, zodat iedereen op de hoogte is van de stappen die gevolgd moeten worden en de verantwoordelijkheden van elke betrokken partij.

6.1.5 Responseplannen

Neem met betrekking tot de responseplannen de volgende acties:

- Maak een stappenplan dat in het responseplan wordt opgenomen, waarin alle stappen vanaf de eerste melding van een incident tot aan de evaluatie zijn beschreven. Dit plan moet duidelijk aangeven welke oplosgroepen/teams verantwoordelijk zijn voor welke fase van het proces;

- Maak een overzicht van het type incidenten die onder het responseplan vallen en identificeer alle interne, en indien van toepassing, externe partijen die betrokken zijn bij het responseplan;

- De organisatie heeft zicht op ICT-systemen en –componenten die essentieel zijn voor kritische bedrijfsprocessen. Voor deze systemen en componenten zijn responsescenario's vastgelegd.

  Deze scenario's beschrijven minimaal:
  - Wat verstaan wordt onder een beveiligingsincident (zie 6.1.1);
  - Hoe wordt de ernst en impact van een incident bepaald en vastgesteld;
  - Welke kritische en belangrijke bedrijfsprocessen zijn afhankelijk van het betreffende systeem of de betreffende systemen;
  - Wie mag besluiten indien er ingegrepen moet worden op de systemen (zie 6.1.3);
  - Wie de externe leveranciers van IT-systemen en informatiebeveiligingsdiensten zijn, waar verantwoordeljikheden liggen en wie ze benadert;
  - Welke maatregelen ter beperking van de impact kunnen worden genomen om verdere verspreiding te voorkomen (containment). Denk daarbij aan het isoleren van specifieke delen van het netwerk of bepaalde informatiesystemen;

  - Welke maatregelen moeten worden genomen om (log)informatie veilig te stellen;
  - Wat is de benodigde communicatie en hoe wordt deze georganiseerd, rekening houdend met de beschikbare communicatiemiddelen. Vooral omdat communicatiesystemen tijdens een cyberincident mogelijk niet toegankelijk zijn.

- Documenteer specifieke verantwoordelijkheden bij een incidentafhandeling door een gedetailleerd overzicht te creëren van de rollen en verantwoordelijkheden van elke betrokkenen, inclusief de Incident Response Manager, teamleden en externe partijen. Dit overzicht moet worden opgesteld in de vorm van een verantwoordelijkheidsmatrix (RACI), waarin duidelijk wordt aangegeven wie verantwoordelijk, geraadpleegd en geïnformeerd moet worden voor elke fase van het incidentresponseproces. Zorg ervoor dat deze documentatie toegankelijk is voor alle medewerkers.

6.1.6 Responsebereik

Neem met betrekking tot het responsebereik de volgende acties:

- Maak een duidelijk overzicht van de (kritieke) IT-systemen in de organisatie en geef aan welke systemen met elkaar verbonden zijn. Gebruik CMDB-tooling, diagrammen of tabellen om de relaties visueel weer te geven zodat het makkelijk te begrijpen is hoe de systemen in elkaar zitten;

- Het is belangrijk om te identificeren welke bedrijfsprocessen als kritiek worden beschouwd. Deze processen zijn bepalend voor de operationele continuïteit van de belangrijkste activiteiten binnen de organisatie. Zodra deze processen in kaart zijn gebracht, kunnen de assets worden geïdentificeerd die essentieel zijn voor de kritieke processen binnen de organisatie. Elke asset wordt vervolgens gecategoriseerd op basis van de mate van kritiek voor het bijbehorende bedrijfsproces, met classificaties als 'kritiek', 'hoog', 'gemiddeld' of 'laag';

- Geef voor elke asset een uitgebreide beschrijving van de impact die kan optreden bij een beveiligingsincident. Dit moet informatie bevatten over de mogelijke gevolgen voor de algehele bedrijfsvoering en het bedrijfsproces waaraan deze asset is gekoppeld, zodat alle betrokkenen de impact op elk systeem begrijpen;

- Beschrijf voor elke (kritiek) bedrijfsproces en/of asset de stakeholders, en contactinformatie, die betrokken en/of geinformeerd moeten worden.

6.1.7 Testen & Oefeningen

Neem met betrekking tot de meldbronnen de volgende acties:

- Organiseer trainingen om het incident response-proces te testen en te oefenen:
  - Maak een lijst van de beveiligingsincidenten die in de afgelopen 12 maanden hebben plaatsgevonden. Het is ook mogelijk een kortere periode van bijvoorbeeld 6 maanden te kiezen;
  - Medewerkers moeten de ruimte krijgen om input te geven over het type incidenten waar zij vinden dat extra training gewenst is omdat het proces daar niet goed werkte;
  - Plan de trainingssessies minimaal een keer per jaar en zorg ervoor dat alle relevante medewerkers aanwezig zijn en deelnemen;
  - Ontwikkel verschillende scenario's op basis van de verzamelde incidenten, waarbij teamleden een incident doornemen om te beoordelen of het proces duidelijk en adequaat is;
  - Leg verbeteringen voor het proces vast in een verslag.
- Zorg ervoor dat de training de basisvaardigheden voor de stappen en procedures duidelijk uitlegt. Geef eenvoudige voorbeelden van elke stap in het proces en laat deelnemers praktische oefeningen doen, zoals het simuleren van een incident en het volgen van de benodigde stappen.

6.1.8 Evaluatie

Neem met betrekking tot de evaluatie de volgende acties:

- Stel een lijst op van de belangrijkste beveiligingsincidenten die het afgelopen jaar hebben plaatsgevonden en verzamel relevante informatie over elk incident.

  Relevante incidentinformatie is:
  - Datum en tijd;
  - Betrokken systemen;
  - Impact op de organisatie inclusief een beschrijving van wat er is gebeurd en hoe elk incident is opgelost;
  - Tickets en rapporten over de incidenten;
  - Verzamelde logs van de incidenten.

- Voer de evaluatie uit door een gestructureerde aanpak te volgen. Voor de evaluatie kan gedacht worden aan de volgende onderwerpen:

  - Was de melding duidelijk en volledig?
  - Was de business impact direct duidelijk?
  - Zijn de juiste stakeholders tijdig geïnformeerd?
  - Zijn er maatregelen genomen om de gevolgen van het incident te beperken?
    - Zo ja, hebben deze het beoogde resultaat opgeleverd?
    - Zo nee, wat waren de redenen waarom geen containment maatregelen te nemen?
  - Waren er aanvullende verbeterpunten of lessen die uit het incident zijn getrokken?

- Organiseer een vergadering om de resultaten van de evaluatie te bespreken en te bepalen welke verbeteracties kunnen worden genomen om het incident response proces te verbeteren (leg de verbeteracties en beslissingen vast in een verslag).

6.2 Niveau 0 naar Niveau 1: Begin naar basis

Doel: De digitale weerbaarheid van de organisatie versterken door een gestructureerde aanpak van beveiligingsincident- & responsemanagement te implementeren. Dit omvat het ontwikkelen van beleid dat specifiek gericht is op digitale weerbaarheid, het vaststellen van duidelijke processen en verantwoordelijkheden, en het realiseren van een basisniveau van monitoring en rapportage.

In de volgende paragrafen is beschreven wat er moet worden geïmplementeerd om niveau 1 te bereiken.

6.2.1 Beleid

Neem met betrekking tot het beleid de volgende acties:

- Evalueer het huidige beleidsdocument en zorg ervoor dat het duidelijke richtlijnen bevat voor het melden van beveiligingsincidenten, inclusief meldpunten en deadlines voor rapportage. Definieer de verantwoordelijkheden van verschillende teams en individuen op een manier die duidelijk maakt wie welke taken heeft, zodat iedereen weet wat er van hen wordt verwacht in geval van een beveiligingsincident;

- Neem in het beleidsdocument een lijst op van de belangrijkste en meest kritieke bedrijfsprocessen van de organisatie. De lijst moet een duidelijke specificatie bevatten van welke diensten als essentieel voor de bedrijfsvoering worden beschouwd. In deze lijst moet ook de impact van mogelijke beveiligingsincidenten op deze diensten worden meegenomen;

- Ontwikkel duidelijke richtlijnen voor het classificeren en prioriteren van beveiligingsincidenten in het beleid. Definieer criteria voor de impact en urgentie van incidenten, zodat medewerkers kunnen bepalen hoe zij moeten reageren;

- Zorg ervoor dat in het beleid is opgenomen dat het ontwikkelen van beleid voor beveiligingsincident-management en response, de analyses van CISO over het informatiebeveiligingsbeleid en het risicobeeld van de organisatie worden geïntegreerd. Beveiligingsincident-management & response moet gebaseerd zijn op het organisatiebeveiligingsbeleid om ervoor te zorgen dat het aansluit bij de specifieke risico's en behoeften van de organisatie.

6.2.2 Proces

Neem met betrekking tot het proces de volgende acties:

- Zorg ervoor dat er een inschalingsmatrix is opgesteld waarmee incidenten op een consistente manier geclassificeerd kunnen worden. Deze matrix moet de urgentie van elk type beveiligingsincident en de mogelijke impact ervan op de organisatie weergeven;

- Bepaal voor elk type beveiligingsincident de urgentie en impact op de organisatie. Bijvoorbeeld, een ransomware-aanval vereist onmiddellijke aandacht (hoog urgentie) en kan aanzienlijke schade toebrengen aan gegevens en de continuïteit van de bedrijfsvoering (hoog impact), terwijl een kwetsbaarheid in een niet aan het internet verbonden server mogelijk minder urgent is;

- Wijs prioriteiten toe aan beveiligingsincidenten op basis van de risicobeoordeling. Koppel de prioriteitscategorieën aan de resultaten van de risicoanalyse. Bijvoorbeeld, een incident dat kan leiden tot een onderbreking van belangrijke bedrijfsprocessen, zoals een DDoS-aanval, kan worden geclassificeerd als prioriteit 1 (hoog risico), terwijl een incident met een lage impact, zoals een spam-e-mail, als prioriteit 4 (laag risico) kan worden ingedeeld;

- Ontwerp een flowchart die medewerkers helpt bij het snel beoordelen van het risico dat een incident met zich meebrengt. Bijvoorbeeld, de flowchart kan beginnen met de vraag: "Is er sprake van een phishing-email?" Afhankelijk van het antwoord kunnen medewerkers worden doorverwezen naar de relevante procedures voor incidentbeheer. Deze flowchart

moet zijn gebaseerd op de classificaties die in de inschalingsmatrix zijn opgenomen, zodat het duidelijk de prioriteit en urgentie van verschillende incidenten weergeeft;

- Ontwikkel een rapportagestructuur voor beveiligingsincidenten en zorg ervoor dat relevante stakeholders op de hoogte worden gehouden. Creëer templates voor rapportages met hierin de incidentstatus, risicobeoordelingen en uitgevoerde actie;

- Stel een schema op voor rapportage aan het management, inclusief IT-management en CISO. Bepaal hoe vaak het management updates moet krijgen over beveiligingsincidenten (bijv. wekelijks of maandelijks) en wie er geïnformeerd moet worden in het management.

6.2.3 Rollen

Neem met betrekking tot de rollen de volgende acties:

- Beschrijf de verantwoordelijkheden en bevoegdheden van elke rol in relatie tot beveiligingsincidenten en de responseprocessen. Zorg ervoor dat elke rol duidelijk weet wie verantwoordelijk is voor welke aspecten van incidentmanagement en response proces;

- Stel verantwoordelijkheden vast voor incidentcoördinatoren die toezicht houden op de voortgang van incidenten. Wijs specifieke personen aan die verantwoordelijk zijn voor het bewaken en opvolgen van incidenten. Bijvoorbeeld: benoem een incidentcoördinator die verantwoordelijk is voor het monitoren van de status van elk incident en het rapporteren over de voortgang aan het management;

- Stel een lijst op van alle belangrijke externe stakeholders die betrokken zijn bij het incident response proces, zoals CSIRT van een externe partij. Beschrijf de verantwoordelijkheden van deze externe partijen. Dit kan inhouden hoe ze samenwerken met interne teams, wanneer ze ingeschakeld worden en welke acties ze ondernemen tijdens een incident;

- Zorg ervoor dat contactinformatie van alle betrokkenen bij incidentresponse (zoals beveiligingsexperts, incidentcoördinatoren en IT-beheerders) altijd beschikbaar is, zelfs wanneer de ICT-systemen van de organisatie niet operationeel zijn. Dit kan bijvoorbeeld worden bereikt door papieren afdrukken van de contactgegevens beschikbaar te stellen of door een digitaal bestand te delen dat toegankelijk is, ongeacht de beschikbaarheid van het bedrijfsnetwerk.

6.2.4 Meldbronnen

Neem met betrekking tot de meldbronnen de volgende acties:

- Zorg ervoor dat medewerkers op de hoogte zijn dat ze bij vermoedens van een beveiligingsincident direct de helpdesk of service desk kunnen bellen, of daar fysiek naartoe kunnen gaan voor ondersteuning. Daarnaast moeten er ook digitale formulieren beschikbaar zijn in het ticketingsysteem dat door de servicedesk wordt gebruikt, zodat medewerkers eenvoudig een melding kunnen indienen;

- Zorg ervoor dat digitale meldingen resulteren in een notificatie bij het IT-beheer team zodat deze opgepakt worden binnen afgesproken en eventueel wettelijk vastgestelde normtijden.

    - Maak bijvoorbeeld gebruik van een e-mailsysteem dat een directe mail stuurt naar de verantwoordelijke teamleden zodra een melding wordt ingediend;
    - Stel normtijden vast waarbinnen meldingen moeten worden beoordeeld. Een voorbeeld hiervan is dat de beoordeling binnen 1 uur na ontvangst moet zijn uitgevoerd, en kritieke incidenten moeten binnen 15 minuten worden opgepakt;

  - Stel in, als een melding na een bepaalde tijd, bijvoorbeeld 30 minuten, nog niet is opgepakt, dat er automatisch een escalatie plaatsvindt naar een senior lid van het IT-beheer team;
  - Stel in, dat er wekelijks rapporten gegenereerd worden die inzicht geven in de (gemiddelde) responsetijden en eventuele achterstanden in het oppakken van meldingen.

- Maak een overzicht van de beveiligingssystemen zoals antimalware en netwerk detectiesystemen die op dit moment aanwezig zijn in de organisatie;

- Zorg ervoor dat er antimalware en netwerk detectiesystemen zoals IDS gecontroleerd zijn zodat de instellingen van netwerk-, cloud- en endpointbeveiligingssystemen automatisch beveiligingsmeldingen genereren wanneer er verdachte activiteiten worden gedetecteerd.

6.2.5 Responseplannen

Neem met betrekking tot de responseplannen de volgende acties:

- Stel een generiek responseplan op dat alle soorten beveiligingsincidenten dekt, met duidelijke richtlijnen voor elke fase van incidentresponse. Definieer specifieke stappen voor het isoleren van een getroffen systeem bij bijvoorbeeld ransomware-aanval en de communicatieprotocollen met betrokken partijen.

  - Beschrijf gedetailleerd de standaardactiviteiten die altijd moeten worden uitgevoerd bij beveiligingsincidenten, zoals het verzamelen van bewijs, het uitvoeren van onderzoek en het rapporteren van incidenten aan relevante autoriteiten (bijvoorbeeld NCSC);
  - Zorg ervoor dat het responseplan procedures bevat voor het escaleren van incidenten naar crisismanagement en het betrekken van leveranciers voor derdelijns support. Stel een checklist op voor het documenteren van de tijdlijn van het incident, de betrokken systemen, en de acties die zijn ondernomen tijdens de response;
  - Definieer de verschillende escalatiemogelijkheden naar crisismanagement en leverancierssupport en de te ondernemen stappen. Bijvoorbeeld: Maak een overzicht van de contactpersonen voor escalatie, inclusief hun rol, verantwoordelijkheden en de specifieke situaties waarin ze gecontacteerd moeten worden;
  - Beschrijf de doelstelling van het responseplan en zorg dat die gerelateerd zijn aan de organisatiedoelstellingen.

6.2.6 Responsebereik

Neem met betrekking tot het responsebereik de volgende acties:

- Zorg ervoor dat bij de beveiligingsincident-afhandeling zowel IT-systemen als bedrijfsprocessen worden meegenomen. Dit betekent dat er niet alleen naar de technische kant wordt gekeken, maar ook naar hoe incidenten de werking van het kritieke bedrijfsprocessen kunnen beïnvloeden;

- Classificeer systemen op risico en impact, als onderdeel van het asset managementproces. Dit houdt in dat je alle systemen in de organisatie bekijkt op de impact en wat de gevolgen kunnen zijn voor de organisatie/afdeling. Door deze classificatie kun je zien welke systemen extra bescherming nodig hebben en welke beveiligingsmaatregelen prioriteit hebben;

- Evalueer het bereik van de responseplannen en pas deze zodanig aan dat minimaal alle kritieke bedrijfsprocessen binnen het bereik vallen.

6.2.7 Testen & Oefeningen

Neem met betrekking tot het testen & oefenen de volgende acties:

- Ontwikkel casestudy's door een aantal relevante voorbeelden van incidenten te bekijken die te maken hebben met leveranciersbeheer en crisismanagement, en organiseer deze rond duidelijke leerdoelen die te maken hebben met het verbeteren van incidentmanagement & response processen. Maak daarna groepsopdrachten waarin deelnemers de situaties analyseren;

- Zorg ervoor dat de training de integratie van belangrijke interne IT-processen zoals probleembeheer, wijzigingenbeheer, assetmanagement, kwetsbaarhedenbeheer en configuratiebeheer behandelt door specifieke casussen te ontwikkelen die deze processen in detail behandelen en voorbeelden van best practices geven, waarbij ook interactieve oefeningen worden opgenomen om te verbeteren in de uitvoering van deze processen;

- Stel scenario’s op van bijvoorbeeld een kwetsbaarheid of aanval die leidt tot systeemuitval, waarbij teams moeten samenwerken om de incidentresponse te coördineren, de oorzaak van de uitval te onderzoeken en een effectief herstelplan te formuleren.

6.2.8 Evaluatie

Neem met betrekking tot de evaluatie de volgende acties:

- Maak een proces waarin de verzamelde best practices worden geïntegreerd in de jaarlijkse evaluatie van beveiligingsincident-management. Dit kan door middel van een review waarbij de huidige processen vergeleken worden met de best practices;

- Implementeer een proces voor het beoordelen van gepubliceerde dreigingsanalyses binnen de sector. Begin met het selecteren van betrouwbare bronnen die regelmatig dreigingsanalyses publiceren, zoals cybersecuritybedrijven en overheidsinstanties. Verzamel de rapporten die zij uitbrengen, bijvoorbeeld elk kwartaal. Analyseer vervolgens de verzamelde gegevens om het huidige dreigingsrisico voor de organisatie te evalueren;

- Evalueer hoe de veranderingen in dreigingsanalyses de instroom van beveiligingsincidenten in de organisatie kunnen beïnvloeden, en pas indien nodig je incidentmanagementprocessen aan om beter voorbereid te zijn op de nieuw geïdentificeerde dreigingen. Dit kan inhouden dat je bestaande processen bijwerkt, nieuwe trainingen organiseert of nieuwe technologieën implementeert of bijwerkt om de beveiliging te versterken, bijvoorbeeld door het bouwen van nieuwe detectieregels.

6.3 Niveau 1 naar Niveau 2: Basis naar uitgebreid

Doel: Een effectief incidentmanagementsysteem opzetten, met een toegankelijk meldpunt voor beveiligingsincidenten, duidelijke verantwoordelijkheden en actuele responseplannen. Daarnaast meer aandacht voor training en bewustwording (testen & oefeningen) zodat elk betrokken rol goed voorbereid is op beveiligingsincidenten.

In de volgende paragrafen is beschreven wat er moet worden geïmplementeerd om niveau 2 te bereiken.

6.3.1 Beleid

Neem met betrekking tot het beleid de volgende acties:

- Ontwikkel en documenteer beleid dat de digitale weerbaarheid van de organisatie waarborgt, met specifieke aandacht voor incidentmanagement en response. Zorg ervoor dat alle relevante eisen uit de Baseline Informatiebeveiliging Overheid (BIO) met betrekking tot beleid over incident management & response aantoonbaar zijn opgenomen in het beleid. Doe dit met behulp van een checklist van de BIO-eisen en koppel deze aan specifieke onderdelen van het beleid om te verifiëren dat aan alle eisen is voldaan;

- Voeg een sectie toe aan het beleidsdocument waarin wordt vastgesteld dat het de verantwoordelijkheid van de CISO is om beveiligingsrisicoanalyses te laten uitvoeren en deze analyses te vertalen naar richtlijnen voor digitale weerbaarheid. Daarnaast is de CISO verantwoordelijk voor het omzetten van de resultaten van deze analyses in specifiek beleid dat de verdere ontwikkeling van het beheer van beveiligingsincidenten en -response ondersteunt. Voor departementale CISO's zijn de taken en bevoegdheden beschreven in artikel 7 en 8 van het Besluit CIO-stelsel Rijksdienst 2021;

- Voeg aan de beleidsteksten over generieke responseplannen toe dat er ook specifieke responseplannen moeten worden ontwikkeld voor unieke of kritieke incidenten, die eigen procedures en maatregelen vereisen.

6.3.2 Proces

Neem met betrekking tot het beleid de volgende acties:

- Evalueer de huidige communicatie- en escalatieprocedures binnen de generieke processen om vast te stellen of deze effectief zijn voor alle incidenttypes. Ontwikkel een communicatieprotocol voor het delen van informatie met betrokken partijen/stakeholders. De organisatie kan de communicatieprocedure uitbreiden met een stappenplan dat, afhankelijk van het type incident, aangeeft wie verantwoordelijk is voor het informeren van het management en de communicatie naar externe stakeholders;

- Voer een analyse uit van de bestaande generieke processen om te identificeren waar de BIO-eisen voor incidentmanagement en response kunnen worden geïntegreerd. Een voorbeeld hiervan is de beoordeling van het proces voor incidentrapportage, waarbij kan worden vastgesteld dat er een specifieke BIO-eis is voor de documentatie van incidenten;

- Bepaal welke unieke of kritieke incidenten specifieke responseplannen vereisen die nog niet zijn gedocumenteerd.
  - Stel templates op voor deze specifieke plannen waarin de stappen, verantwoordelijkheden en communicatieprotocollen zijn vastgelegd;
  - Zorg ervoor dat de specifieke processen, voor bijvoorbeeld prio 1 incidenten, bekend zijn bij de medewerkers die betrokken zijn bij het verwerken/oplossen van meldingen.

6.3.3 Rollen

Neem met betrekking tot de rollen de volgende acties:

- Benoem een verantwoordelijke voor het meldpunt van kwetsbaarheden binnen de organisatie. Dit kan een afdeling zijn die al verantwoordelijk is voor IT-ondersteuning of beveiliging.

  - Ontwikkel duidelijke richtlijnen en procedures voor het indienen van kwetsbaarheden, inclusief hoe en waar meldingen moeten worden gedaan.

- De Information Security Officer (ISO), in samenwerking met de Chief Information Security Officer (CISO), is verantwoordelijk voor het ontwikkelen van duidelijke en gedetailleerde responseplannen voor verschillende soorten beveiligingsincidenten. Deze plannen bevatten alle relevante stappen die nodig zijn om te reageren op incidenten, van detectie en identificatie tot afhandeling en rapportage;

- Zorg ervoor dat alle betrokkenen bij het incidentresponseproces op de hoogte zijn van hun verantwoordelijkheden met betrekking tot informatiebeveiliging. Dit moet duidelijk worden vermeld in de functieomschrijvingen en beleidsdocumenten. Daarnaast moet in de hele organisatie bekend zijn wie of welke afdeling benaderd kan worden voor informatiebeveiligingsincidenten.

6.3.4 Meldbronnen

Neem met betrekking tot de meldbronnen de volgende acties:

- Implementeer een eerste versie van een Security Operations Center (SOC) waarbij systemen beveiligingsmeldingen verzamelen en automatisch een beveiligingsincident melding aanmaakt.
  - Configureer de securityevent logging zodat deze een bron is voor detectie binnen de security monitoring;
  - Selecteer en configureer de juiste software of tools om meldingen effectief te verzamelen en door te sturen naar een SIEM.

- Bepaal de criteria en drempelwaarden die gebruikt moeten worden om meldingen te classificeren op basis van type incident en urgentie binnen SOC tooling.
  - Verzamel gegevens over eerdere meldingen en incidenten. Analyseer deze gegevens om trends te identificeren, zoals veelvoorkomende type incidenten en hun impact op de organisatie;
  - Bepaal wat de meeste prioriteit heeft, zoals het verminderen van false positives/negatives, het verbeteren van de responsetijd of het prioriteren van incidenten;
  - Stel drempelwaarden in op basis van de ernst en type van incidenten. Dit kan bijvoorbeeld inhouden dat meldingen met een bepaalde score automatisch als hoog risico worden geclassificeerd;
  - Zorg ervoor dat de criteria en drempelwaarden goed gedocumenteerd zijn.

6.3.5 Responseplannen

Neem met betrekking tot de responseplannen de volgende acties:

- Stel vast welk type incidenten een specifiek responseplan nodig heeft. Er kan gekeken worden naar het volgende om te bepalen wanneer een specifiek responseplan gewenst is:
  - Wanneer de dreiging en het risico aanzienlijk zijn, kan een generiek plan niet voldoende zijn om effectief te reageren. Er is een gerichte aanpak nodig die rekening houdt met de specifieke omstandigheden van het incident;
  - Er zijn best practices beschikbaar die het mogelijk maken om een specifiek responseplan te ontwikkelen. Deze best practices bieden richtlijnen die zijn afgestemd op de unieke kenmerken van bepaalde incidenten.

- Ontwerp en documenteer specifieke responseplannen voor elk van de geïdentificeerde incidenten. Zorg ervoor dat deze plannen zijn afgestemd op de unieke kenmerken van elk type incident en gebruik maken van het generieke beveiligingsresponseplan als basis.
  - In elk responseplan moet een strategie worden opgenomen voor containment. Dit houdt in dat duidelijk moet worden vastgelegd welke acties moeten worden ondernomen om de impact van een incident te beperken, wanneer er wordt overgegaan op containment en wie bevoegd is dit uit te voeren;
  - Integreer richtlijnen in de responseplannen voor het veiligstellen van informatie die nodig is voor forensisch onderzoek. Dit omvat procedures voor het maken van een

kopie van data, het bewaren van bewijs en het minimaliseren van gegevensverlies.

6.3.6 Responsebereik

Neem met betrekking tot het responsebereik de volgende acties:

- Zorg ervoor dat er (ook) een risicoanalyse wordt uitgevoerd voor minder kritieke bedrijfssystemen en dat de resultaten hiervan worden besproken. Dit is belangrijk om vast te stellen of deze systemen voldoende zijn afgedekt door het generieke incidentresponseplan of dat ze een apart responseplan nodig hebben.
    - Begin met het in kaart brengen van de bedrijfssystemen die als minder kritisch worden beschouwd;
    - Verzamel gegevens over deze systemen om inzicht te krijgen in de impact van een cyberaanval op de vertrouwelijkheid, integriteit en beschikbaarheid;
    - Documenteer, op basis van risicoanalyses, de mogelijke bedreigingen voor elk systeem;
    - Evalueer de impact en urgentie van elke bedreiging op de systemen. Hiervoor kan een inschalingsmatrix worden gebruikt;
    - Bepaal welke systemen worden gedekt door het generieke responseplan. Als het generieke plan niet geschikt blijkt te zijn voor bepaalde systemen, bijvoorbeeld omdat de acties in het plan teveel impact hebben op minder kritieke systemen, evalueer dan of het noodzakelijk is om het generieke plan aan te passen of dat er een specifiek responseplan moet worden ontwikkeld voor die systemen.

- Update de responseplannen door niet alleen het worst-case scenario op te nemen, maar ook andere mogelijke scenario's met een minder grote impact, die nog steeds relevant zijn. Dit kan bijvoorbeeld inhouden dat je rekening houdt met een (tijdelijke) verstoring van systemen die niet betrokken zijn bij kritieke bedrijfsprocessen.
    - Breng andere mogelijke situaties in kaart die zich kunnen voordoen die minder ernstig zijn. Bijvoorbeeld tijdelijke verstoringen van systemen die niet direct zijn gekoppeld aan kritieke bedrijfsprocessen.

- Controleer of de bestaande responseplannen voor zowel grote als kleine beveiligingsincidenten zijn afgestemd op de informatieketen, leveranciers en partners.
    - Breng in kaart welke externe partijen betrokken zijn bij de informatie- en waardeketen van de organisatie. Hoe wordt de rol van externe partijen in de incidentresponse behandeld.

6.3.7 Testen & Oefeningen

Neem met betrekking tot het testen & oefeningen de volgende acties:

- Plan en organiseer op structurele basis tabletop oefeningen met alle relevante stakeholders en medewerkers;

- Maak realistische en relevante scenario's die de deelnemers kunnen gebruiken om responseplannen te testen. Zorg ervoor dat deze scenario’s bestaan uit zowel grote als kleine incidenten:
    - Maak een lijst van de belangrijkste teams en personen binnen de organisatie die betrokken zijn bij beveiligingsincidenten, zoals IT-Beheer, IT-security team, communicatie en management;
    - Maak een lijst van alle externe partners en organisaties die deel uitmaken van de informatie- en waardeketen, zoals leveranciers en partners;
    - Plan oefeningen waarin zowel interne teams als externe partners deelnemen. Dit kan helpen om de samenwerking en communicatie tijdens incidenten te verbeteren.

6.3.8 Evaluatie

Neem met betrekking tot het beleid de volgende acties:

- Maak een overzicht van de BIO-richtlijnen die meegenomen moeten worden in de evaluatie van processen voor beveiligingsincident-management en -response.
    - Stel een lijst samen van relevante BIO-richtlijnen;
    - Vergelijk de huidige processen met de eisen van de BIO en leg potentiële verbeteringen vast;
    - Documenteer de bevindingen en formuleer aanbevelingen voor verbeteringen.

- Beveiligingsincidenten van het afgelopen jaar worden bekeken om te leren hoe de afhandeling van incidenten. Voer verbeteringen door in de processen en responseplannen.
    - Verzamel gegevens over alle beveiligingsincidenten die zich in de afgelopen 12 maanden hebben voorgedaan;
    - Voer een evaluatie uit waar je tenminste het volgende bespreekt:
        - Is het incidentproces gevolgd?
        - Zijn de prestatie indicatoren gehaald?
        - Waren de classificaties correct?
        - Welke escalatie heeft plaatsgevonden?

- De processen voor beveiligingsincident-management en -response worden geëvalueerd op hun samenwerking met de informatie- en waardeketen.
    - Organiseer bijeenkomsten met stakeholders in de keten die zijn geraakt bij een incident;
    - Bespreek tenminste het volgende:
        - Welke communicatie heeft plaatsgevonden met partijen in de informatie- en waardeketen en was deze communicatie tijdig?
        - Wat kan er de volgende keer beter gedaan worden?
        - Hebben de incident response plannen gewerkt? Wat kan volgende keer beter?

6.4 Niveau 2 naar Niveau 3: Uitgebreid naar risico geoptimaliseerd

Doel: Het opzetten van een risicogeoptimaliseerd beveiligingsincident-management & response proces met ondersteuning van een Cyber Defense Center.

In de volgende paragrafen is beschreven wat er moet worden geïmplementeerd om niveau 3 te bereiken.

6.4.1 Beleid

Neem met betrekking tot het beleid de volgende acties:

- Het incidentmanagement en responsebeleid moet geformaliseerd zijn, met specifieke procedures en verantwoordelijkheden die zijn afgestemd op de bredere managementdoelstellingen van de organisatie. Dit beleid dient te waarborgen dat incidenten effectief worden geïdentificeerd, gemitigeerd, gerapporteerd en geëvalueerd, terwijl het managementteam actief betrokken wordt bij de ontwikkeling en verbetering van het beleid.
    - Zorg ervoor dat er duidelijke kaders worden vastgelegd met betrekking tot het uitvoeren van evaluaties. Deze evaluaties omvatten ook onderzoeken naar hoe incidenten kunnen worden voorkomen en welke lessen kunnen worden getrokken om soortgelijke incidenten in de toekomst te voorkomen of de kans daarop te minimaliseren;
    - Neem in het beleid concrete kaders op met betrekking tot het implementeren van systemen voor het verzamelen en analyseren van gegevens over incidenten en de effectiviteit van de response.

- Neem in het beleid concrete kaders op met betrekking tot het identificeren van de benodigde middelen voor de uitvoering van het incidentmanagement- en responsebeleid of het verder verbeteren van de uitvoering. Er moet een analyse uitgevoerd worden om te bepalen welke middelen essentieel zijn voor een effectieve response op incidenten. Deze bevindingen worden met het management gedeeld, zodat prioriteiten kunnen worden gesteld en de juiste investeringen kunnen worden gedaan om de effectiviteit van het beleid te waarborgen.

6.4.2 Proces

Neem met betrekking tot het proces de volgende acties:

- Zorg ervoor dat de processen voor beveiligingsincident-management en response systematisch zijn ingericht en regelmatig worden geëvalueerd. Door periodieke evaluaties kunnen tekortkomingen of potentiële verbeterpunten worden geïdentificeerd.
    - Voer bijvoorbeeld elke 6 maanden een evaluatie uit van de incidentresponseprocessen om te controleren of ze nog steeds effectief zijn en voldoen aan de huidige bedreigingen voor de organisatie.

- Beveiligingsincident-management moet worden geïntegreerd met de risicomanagement- en continuïteitsmanagementstrategieën van de organisatie. Dit houdt in dat alle relevante risico's en incidenten samen worden beheerd. Deze integratie zorgt ervoor dat de organisatie snel kan reageren op beveiligingsincidenten en de continuïteit voor alle relevante bedrijfsprocessen.
    - Volg een gestructureerde aanpak zoals ITIL of COBIT, bij het opzetten van beveiligingsgovernance en -processen.

- Zorg ervoor dat informatieketens binnen de organisatie in kaart zijn gebracht, en alle betrokken stakeholders actief worden betrokken bij het beveiligingsincident-management. Door deze samenwerking wordt een gecoördineerde response op beveiligingsincidenten mogelijk gemaakt.
    - Organiseer bijeenkomsten met partijen uit de informatieketen en maak afspraken om invulling te geven aan hun belangen.

6.4.3 Rollen

Neem met betrekking tot de rollen de volgende acties:

- Benoem beveiligingsspecialisten binnen alle IT-domeinen in de organisatie, en zorg ervoor dat incidentmanagement een verantwoordelijkheid is van alle medewerkers en leveranciers.
  - Zorg ervoor dat de volgende rollen al zijn ingevuld: ISO (Information Security Officer), CISO (Chief Information Security Officer) Security incident- en responsemanager (SIRM) Security incident responder, Security analist;
  - Maak een lijst van alle relevante IT-domeinen binnen de organisatie. Stel voor elk domein vast welke specifieke vaardigheden en kennis nodig zijn om als beveiligingsexpert te functioneren;
  - Benoem per domein één of meerdere medewerkers en communiceer dit intern;
  - Betrek de beveiligingsspecialisten bij alle lagen van de IT-governance.

- Zorg ervoor dat de verantwoordelijkheden voor informatiebeveiliging en incidentmanagement gespecificeerd zijn voor alle leveranciers en partners.
  - Raadpleeg het beleid dat de kaders specificeert voor de eisen en verwachtingen voor leveranciers en partners met betrekking tot informatiebeveiliging- en incidentmanagement.

- Wijs een coördinator aan die verantwoordelijk is voor het beheer van beveiligingsincidenten binnen het ecosysteem (incl. externe partners).
  Zorg ervoor dat de coördinator nauw samenwerkt met de Security Incident- en Responsemanager en de Chief Information Security Officer (CISO).

- Zorg ervoor dat lijnmanagers verantwoordelijk zijn voor de communicatie van de responseplannen binnen de keten en dat zij het proces actief managen.
  - Definieer duidelijk welke lijnmanagers verantwoordelijk zijn voor de communicatie van de responseplannen en zorg ervoor dat ze goed geïnformeerd zijn over de inhoud en doelstellingen van deze plannen;
  - Indien nodig; ontwikkel een communicatieplan dat beschrijft hoe informatie over de responseplannen binnen de keten zal worden gedeeld. Dit plan moet ook de frequentie, gebruikte kanalen en de betrokken stakeholders specificeren.

6.4.4 Meldbronnen

Neem met betrekking tot de meldbronnen de volgende acties:

- Automatiseer het proces voor de classificatie en prioritering van beveiligingsincidenten in het incidentmanagementsysteem.
  - Configureer het systeem om automatisch beveiligingsincidenten te classificeren op basis van vooraf gedefinieerde criteria (impact & urgentie);
  - Wanneer een melding binnenkomt, wordt automatisch de classificatie van de betrokken asset weergegeven.

- Zorg ervoor dat de monitoringfunctie meldingen kan verrijken met informatie over de architectuur van de organisatie en configuratie van de systemen. Bijvoorbeeld met visualisatietools.
  - Zorg ervoor dat SOC-analisten toegang hebben tot architectuurdiagrammen of netwerktekeningen.

- Definieer duidelijke protocollen voor communicatie en samenwerking tussen de SOC en CSIRT;
  - Evalueer bestaande richtlijnen over hoe en wanneer incidenten moeten worden gemeld bij CSIRT;
  - Bepaal welke communicatiekanalen gebruikt worden;
  - Ontwikkel een gestandaardiseerd format voor rapportages;
  - Voer regelmatig tabletop-oefeningen of simulaties uit waarbij zowel SOC- als CSIRT-teams betrokken zijn, om de samenwerking en response op incidenten te

verbeteren.

6.4.5 Responseplannen

Neem met betrekking tot het beleid de volgende acties:

- Zorg ervoor dat de generieke en specifieke responseplannen zijn afgestemd op de informatiebeveiligingsrisico's voor de organisatie.
  - Maak een lijst van security use-cases die de meest waarschijnlijke en impactvolle risico's bevatten voor de organisatie;
  - Evalueer de bestaande responseplannen met de security use-cases om te bepalen welke risico's of acties niet zijn opgenomen;
  - Pas de bestaande responseplannen aan om ze beter af te stemmen op de security use-cases.

- Zorg ervoor dat de response plannen de volgende elementen bevatten:
  - Het beperken van de impact van het incident. Documenteer de stappen die zijn genomen bij een incident. Bijvoorbeeld het isoleren van getroffen systemen, blokkeren van kwaadaardig verkeer, en communiceren met relevante stakeholders;
  - Het vaststellen van het doel van de aanvaller. Beschrijf de resultaten van forensische analyses en logmonitoring om te begrijpen welke systemen of gegevens het doelwit waren;
  - De identiteit van de aanvaller. Hiervoor kan bijvoorbeeld gebruik gemaakt worden van threat intelligence;
  - De methodes die door de aanvaller gehanteerd worden. Hiervoor kan gebruik worden gemaakt van frameworks zoals MITRE ATT&CK om aanvallersmethoden te categoriseren en te beschrijven;
  - Het herstel van de cyber-veiligheid van de omgeving. Beschrijf stappen voor het herstellen van systemen, inclusief back-up- en herstelprocedures;
  - Het herstel van de afgesproken dienstverlening niveaus.

6.4.6 Responsebereik

Neem met betrekking tot het responsebereik de volgende acties:

- Bepaal of de bestaande responseplannen een geformaliseerde ketenaanpak bevatten en of deze plannen zijn gecommuniceerd over de keten.
  - Evalueer de bestaande responseplannen en controleer of er een geformaliseerde ketenaanpak is opgenomen;
  - Voer gesprekken met de relevante partijen binnen de keten om protocollen op te stellen voor het opnemen van een geformaliseerde ketenaanpak in de responseplannen, mocht deze nog ontbreken;
  - Zorg ervoor dat, wanneer het responseplan de gehele keten raakt, dit proactief wordt gedeeld met alle betrokken partners en dat er een gezamenlijke overeenstemming wordt bereikt over de uitvoering.

6.4.7 Testen & Oefenen

Neem met betrekking tot het beleid de volgende acties:

- Voer regelmatig testen en oefeningen uit om de effectiviteit van de responseplannen te evalueren. Gebruik hiervoor daadwerkelijk voorgevallen incidenten als referentie.
  - Neem ook oefeningen op waarin escalatie naar crisismanagement en ondersteuning van leveranciers wordt geïntegreerd.

- Zorg ervoor dat alle relevante medewerkers deelnemen aan de geplande oefeningen, zoals ART of TIBER, en dat de leerpunten zorgvuldig worden vastgelegd.
  - Maak gebruik van professionele trainers om de training te begeleiden.

6.4.8 Evaluatie

Neem met betrekking tot de evaluatie de volgende acties:

- Zorg ervoor dat elk beveiligingsincident binnen 30 dagen na herstel wordt geëvalueerd om lessen te trekken en toekomstige incidenten te voorkomen
    - Automatiseer het aanmaken van meldingen (binnen 30 dagen) na sluiten van een incident om ervoor te zorgen dat de evaluatie niet wordt vergeten;
    - Plan afhankelijk van de impact van het incident bijeenkomen met relevante stakeholders om het incident te bespreken en verbeterpunten te identificeren.

- Zorg ervoor dat de evaluatie altijd plaatsvindt na een significante wijziging in de dreigingen of kwetsbaarheden binnen het ecosysteem, zodat de responseplannen en alle relevante processen actueel blijven.
    - Zorg voor automatische meldingen of updates over veranderingen in het dreigingslandschap. Dit kan bijvoorbeeld door rapporten van organisaties die zich bezighouden met cyberveiligheid, zoals het Nationaal Cyber Security Centrum (NCSC) en de European Union Agency for Cybersecurity (ENISA). Daarnaast kunnen automatische e-mails of feeds ingesteld worden vanuit threat intelligence platforms of websites om ervoor te zorgen dat deze belangrijke informatie over nieuwe aanvalstechnieken of kwetsbaarheden vanzelf binnenkomt;
    - Wanneer een significante wijziging wordt vastgesteld, plan dan een evaluatiebijeenkomst met relevante stakeholders om de impact op de beveiligingsprocessen te bespreken.

- Zorg ervoor dat alle trainingsresultaten en oefeningen leiden tot een evaluatie van de informatiebeveiligingsprocessen.
    - Evalueer op basis van de resultaten welke verbeteringen nodig zijn in de informatiebeveiligingsprocessen;
    - Documenteer de bevindingen en voorgestelde verbeteringen en zorg ervoor dat deze effectief worden geïmplementeerd.

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