TLP:GREEN

IR-1 CAPABILITY ASSESSMENT TOELICHTING

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	30-06-2025	Foutcorrecties 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)" onder Incident Response Readiness
Incident Response 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
Woordenboek Cyberveilig Nederland	Woordenboek - Cyberveilig Nederland
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

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

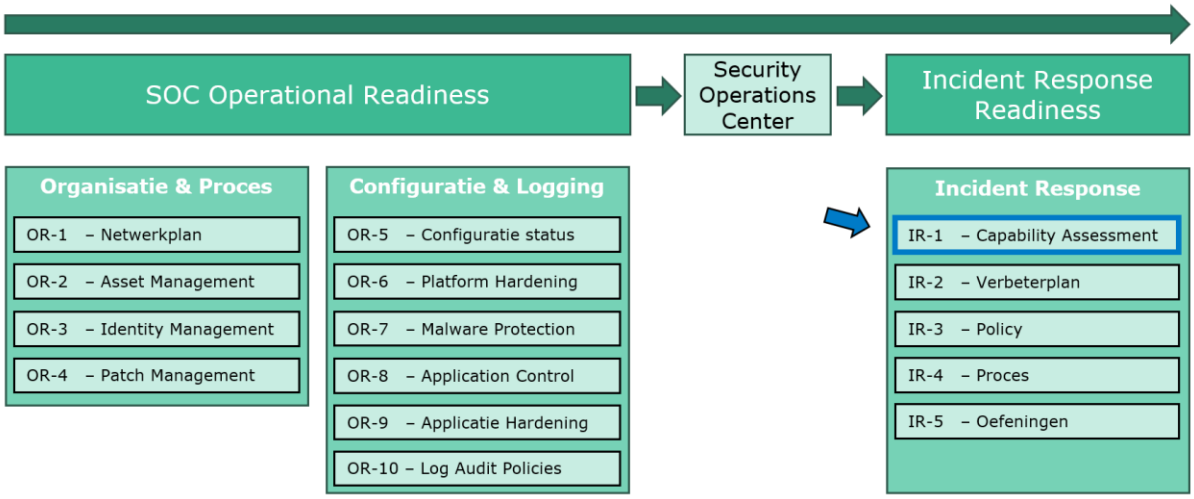
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

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

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

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



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

De documenten onder IR-1 Capability Assessment bestaan uit:

- Capability Assessment toelichting (**Dit document**)
  PDF document voorziet in een toelichting op het "Capability Assessment"

- Capability Assessment
  Excel document waarmee de organisatiestatus ten aanzien van Incident Response kan worden bepaald.

3 Leeswijzer

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

3.1 Doel van dit document (Capability Assessment Toelichting)

Dit document bevat een toelichting op het gebruik van het Incident Response Capability Assessment, waarmee organisaties inzicht krijgen in hun volwassenheidsniveau op het gebied van beveiligingsincident-management en incident response. Daarnaast geeft het document inzicht in de opzet en structuur van het assessment. Dit inzicht helpt ook bij het toepassen van overige Incident Response-producten.

3.2 Opbouw van het assessment

Het capability-assessment is ontwikkeld als onderdeel van de VSSR-miniproducten en ondersteunt organisaties bij het verbeteren van hun digitale weerbaarheid tegen beveiligingsincidenten. Het richt zich op de onderdelen van Incident Response die een organisatie op orde moet hebben om adequaat te kunnen reageren op cyberincidenten en -dreigingen.

Verschillende kaders en richtlijnen, zoals de Baseline Informatiebeveiliging Overheid (BIO), het NIST Cybersecurity Framework (CSF) en de NIS2-richtlijn, bieden richtlijnen die 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. Het capability assessment is, mede, ontwikkeld op basis van deze raamwerken & richtlijnen.

Het assessment bestaat uit:

- **Acht thema's**: Beleid, Proces, Rollen, Meldbronnen, Responseplannen, Responsebereik, Testen & Oefeningen, en Evaluatie;
- **Vier niveaus** van volledigheid: van Niveau 0 (Begin) tot Niveau 3 (Risico-geoptimaliseerd).

Het assessment is geen platformmodel. Dat betekent dat een organisatie niet noodzakelijkerwijs alle thema's op hetzelfde niveau zal hebben. Per thema kan het volwassenheidsniveau verschillen, afhankelijk van context, risicoafweging en prioriteiten.

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 plan	IT-systemen met business	Ja / Nee	Na crisis
Niveau 2 (Uitgebreid)	Instru-menteel	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	Red Team	Altijd

Tabel 1 Capability-niveaus matrix

Deze indeling maakt het mogelijk om verbeteracties op te splitsen in compacte werkpakketten die binnen enkele weken uitvoerbaar zijn, zonder dat hiervoor grootschalige projecten of programma's nodig zijn.

Door het uitvoeren van dit assessment krijg je inzicht in:

- De huidige stand van zaken per thema;

- De benodigde stappen om door te groeien naar een hoger niveau;
- Knelpunten of hiaten in processen, rollen of technische inrichting.

3.2.1 Indeling in niveaus

Het assessment kent vier niveaus (0 t/m 3). Niveau 0 representeert een basisniveau dat in de praktijk bij vrijwel elke organisatie met ICT-systemen aanwezig zou moeten zijn. Niveau 2 komt overeen met BIO-compliance op het gebied van Incident Response. Omdat de stap van niveau 0 naar 2 relatief groot is, is een tussenstap op niveau 1 toegevoegd. Niveau 3 is bedoeld voor organisaties die verder willen groeien naar een risico gestuurde benadering van incident response.

Een uitgebreide beschrijving van de niveaus is te vinden in hoofdstuk 0.

3.3 Gebruik van het assessment

Het assessment is beschikbaar als Excelsheet (zie paragraaf 1.2, Incident Response – Capability Assessment).

De Excelsheet bevat:

- Een informatieblad;
- Per thema een apart tabblad;
- Een dashboard-tabblad.

Vul voor elk thema het bijbehorende tabblad in. Elk tabblad bevat drie vragen per niveau. Wanneer alle drie de vragen van een niveau met ‘ja’ worden beantwoord, wordt dat niveau als behaald beschouwd.

Het Dashboard toont de resultaten in een matrix met percentages per thema en niveau. Ook bevat het dashboard een progressiebalk per niveau. Deze balk toont pas voortgang zodra alle thema’s van het onderliggende niveau zijn behaald.

Een korte uitleg over de werking van het assessment is ook te vinden in het Info-tabblad van de Excelsheet.

3.4 Aan de slag

Gebruik deze toelichting altijd in combinatie met het Excelbestand IR1 – Capability Assessment. Het is aan te raden het assessment uit te voeren in workshopvorm, met betrokken functionarissen. Bewijsstukken zijn niet vereist – het gaat om het gezamenlijk vaststellen van het huidige volwassenheidsniveau en het identificeren van relevante verbeterslagen.

4 Assessment introductie

Dit kennisdocument beschrijft een capability-assessment van de organisatie op het gebied van beveiligingsincident-management & response. Bij beveiligingsincidenten gaat het hier om de digitale weerbaarheid van de organisatie. Fysieke beveiliging is dan ook geen onderdeel van het assessment. Dit document is een toelichting op het Excel document "IR1- Incident Response - Capability Assessment" (Zie 1.2 Referenties).

We geven eerst aan wat een capability-assessment is en wat het niet is. Vervolgens geven we aan wat het doel is van het assessment en hoe het gebruikt kan worden in de opzet van de weerbaarheid bij gebruik van een SOC-dienst.

4.1 Wat is een capability-assessment?

Een capability-assessment is een onderzoek wat inzicht geeft in de capabilities of het vermogen van een organisatie om, in dit geval, beveiligingsincident-management & response effectief te kunnen inzetten om weerbaar te zijn tegen cyberaanvallen en andere verstoringen op het gebied van informatiebeveiliging.

4.2 Welke doelen heeft het assessment?

Het doel van het assessment is om een analyse te maken van de mate waarin uw organisatie in staat is om adequaat opvolging te geven aan informatiebeveiligingsincidenten. Het uitgangspunt is dat het proces gebruik maakt van informatie dat zowel door gebruikers als door een monitoringproces wordt aangeleverd.

Het doel is niet om vast te stellen of uw organisatie voldoende volwassenheid heeft op dit vlak en ook niet om vast te stellen of uw volledig bent in het afnemen van alle diensten die een volwaardig SOC kan leveren. Vergelijk het met een auto die u gebruikt om een vervoersprobleem op te lossen. Met het capability-assessment kunt u vaststellen of u in staat bent de auto effectief te besturen. Er wordt niet vastgesteld of u zuinig rijdt, of u snel bent, of u een stadsauto heeft of een rally-auto.

Het doel van het assessment wordt bereikt door inzicht te verschaffen in eventuele omissies in het management & responseproces waardoor uw organisatie ook inzicht krijgt in de te nemen acties om deze omissies op te lossen.

4.3 Onderscheid tussen gewoon incidentmanagement en beveiligingsincident-management & response

Een gehanteerde definitie van het incidentmanagement-proces is "het proces van het herstellen van het afgesproken dienstenniveau".

Strikt genomen geldt dat ook voor beveiligingsincident-management & response. Een cyberaanval met bijvoorbeeld ransomware is ook een verstoring van de het afgesproken dienstenniveau en ook daar wordt alles in het werk gesteld om het afgesproken dienstenniveau te herstellen. De herstelactie is niet meer dan de response die volgens een plan wordt uitgevoerd. Nader onderzoek naar de oorzaak gebeurt dan in het probleemmanagementproces en de verbeteractie om dit in de toekomst te voorkomen wordt weer met changemanagement uitgevoerd.

Beveiligingsincidenten hebben een aantal specifieke elementen in deze processen die rechtvaardigen er een apart proces of aparte processtappen voor te definiëren.

Hierbij moet gedacht worden aan:

- Specifieke rollen die meedoen in het proces zoals de rollen binnen het SOC, de Information Security Officer (ISO), de Corporate Information Security Officer (CISO), de beveiligingsbeambte.
- Specifieke organisaties die meedoen in het proces zoals het NCSC, de Bevoegde Autoriteit (Competent Authority) in het kader van de meldplicht uit de NIS2, het van toepassing zijnde Cyber Security Incident Response Team (CSIRT), de Autoriteit Persoonsgegevens (AP) en natuurlijk het SOC-team.
- Specifieke stappen in het proces zoals het veiligstellen van informatie in het kader van noodzakelijk forensisch onderzoek, de plannen tot het beperken van de impact van het incident en het verwijderen van software die een hacker achterlaat op de systemen.
- De onzekerheid over de werkelijke reikwijdte van een incident en de response; het zichtbare effect kan het spreekwoordelijke topje van de ijsberg zijn en systemen die nog steeds het afgesproken dienstenniveau leveren kunnen wel al geïnfecteerd zijn. De responseplannen moeten dus met een grote mate van onzekerheid uit de voeten kunnen.
- Beveiligingsincidenten hebben niet altijd een directe voelbare impact op de gebruikers van ICT-systemen. Regulier incidentmanagement is hierdoor niet altijd in staat om beveiligingsincidenten met de juiste prioriteit op te pakken. Een proces dat specifiek gericht is op informatiebeveiligingsincidenten kan ervoor zorgen dat beveiligingsincidenten met de juiste prioriteit worden behandeld.

4.4 Hoe is het capability-assessment opgezet?

Het assessment is opgezet in een beperkt aantal niveaus die te onderscheiden zijn binnen een organisatie. Het onderscheid wordt gemaakt door de elementen en hun samenhang die we per niveau hebben ogenomen. Elementen uit bestaande raamwerken voor IT-governance zijn gebruikt om het assessment vorm te geven. Dit zijn onder andere:

- De Basis Informatiebeveiliging Overheid (BIO) waarbij een van de niveaus uit het assessment ook het niveau van compliance aan de BIO reflecteert.
- De NIST Cyber Security Framework (CSF) versie 2.0 wat de huidige internationale standaard is om cyberweerbaarheid in een organisatievorm te geven en waarbij het uitgangspunt is dat niet alles is te voorkomen met preventieve maatregelen en er dus een balans moet zijn met maatregelen die in de detectie liggen (het SOC) en in de acties volgend op een incident (de response). De belangrijkste elementen die in het NIST CSF zijn beschreven voor incident management en responsemanagement zijn opgenomen in de niveaus.

Deze elementen in de niveaus zijn zodanig opgenomen dat een BIO-compliant organisatie op niveau 2 zal uitkomen. Niveau 0 vertegenwoordigt een overheidsorganisatie met een aantal elementen die we verwachten aan te treffen bij organisaties met een beperkte volwassenheid op informatiebeveiliging. Niveau 1 is gepositioneerd tussen niveau 0 en niveau 2 zodat de activiteiten om te komen tot niveau 3 in 2 stappen te overbruggen zijn. Niveau 3 gaat uit van een organisatie die een stap verder is dan BIO-compliant en op basis van haar risicoperceptie en risico-acceptatie al volgende stappen heeft gezet.

De elementen die gekozen zijn in de capability-assessment zijn terug te vinden in de andere kennisdocumenten voor Incident Response.

De gekozen elementen hebben een relatie tot elkaar en hebben ook een logische volgorde. Zo hebben de testen en oefeningen een relatie tot de processtappen en de responseplannen die bij het niveau horen. De volgorde begint bij het hebben van beleid, gevolgd door het inrichten van het proces, en eindigt bij het evalueren van de effectiviteit.

4.5 Hoe en wanneer kun je het capability-assessment uitvoeren?

Het assessment kan uitgevoerd worden in een kort projectverband waarbij één persoon de leiding heeft en van het management het mandaat heeft gekregen de benodigde personen te benaderen en in te zetten in een workshop om het assessment uit te voeren. De benodigde personen zijn te bepalen door de rollen die benoemd zijn per kenmerk van het beveiligingsincident-management & responseproces. Het is de bedoeling om een indruk te krijgen op welk niveau je overwegend zit zodat je in staat bent te bepalen welke activiteiten je moet uitvoeren om op het volgende niveau te komen. Daarom is het niet nodig de personen te vragen om met bewijsvoering te komen om aan te tonen of een maatregel uit het assessment wel of niet geïmplementeerd is.

Een voorbeeld-werkwijze is dat je de functionarissen die het meeste passen bij de beschreven rollen uitnodigt voor een workshop en gezamenlijk bepaalt waar je staat. Een workshop kan binnen een dagdeel uitgevoerd worden. Het beeld wat dan ontstaat, kan na uitwerking nog geverifieerd worden door de deelnemers en de personen die niet konden meedoen aan de workshop. Alle vragen gaan over een 3-tal aan te treffen inrichtingselementen. Je voldoet aan een niveau wanneer aan alle elementen op dat niveau invulling is gegeven.

In algemene zin is het verstandig het assessment ook uit te voeren aan de start van een verandertraject en opnieuw aan het einde daarvan. Hierdoor ontstaat duidelijkheid of de beoogde verandering ook gehaald is en wordt ook een nieuwe verbeterslag geïnitieerd. Wanneer het verandertraject meerdere jaren beslaat is het ook verstandig het assessment te herhalen op een tussenliggend moment zodat duidelijk wordt of het verandertraject nog steeds op koers ligt.
Ook kan het assessment gebruikt worden als voorbereiding op de begrotingsplanning zodat op basis van het plan een inschatting gemaakt kan worden van de bijbehorende kosten.

4.6 Gebruik van het assessment-resultaat

Het resultaat van het capability-assessment geeft een aanwijzing over waar de organisatie zich op moet richten om effectief op te kunnen treden bij beveiligingsincidenten waardoor de weerbaarheid zal vergroten. Op basis van waar de organisatie staat (welk niveau in ruime mate wordt gehaald) kan bepaald worden welke activiteiten gepland moeten worden in de komende periode om naar een volgend niveau te komen.

De kenmerken van een niveau zijn bewust niet voorzien van een weging. Het is aan de organisatie zelf om te bepalen welke kenmerken als belangrijker worden gezien en meer aandacht behoeven. Door dat wel in overweging te nemen wordt de planning organisatiespecifiek. Een weging zou ten minste bepaald moeten worden door de risicoafweging die een organisatie gemaakt heeft.
Het assessment geeft een aanwijzing wat je moet veranderen in de organisatie maar het geeft geen aanwijzing ten aanzien van het verandervermogen in de organisatie en ook niet de capaciteit die nodig is van de verandermanager of projectleiding. Het is wel belangrijk hier over een beeld te vormen en niet te proberen te veel in een keer te realiseren. Groei in een periode van één niveau is daarbij een uitgangspunt. Als de organisatie redenen heeft om sneller of langzamer te gaan dan is het advies daar specifieke maatregelen voor te nemen.

Wanneer de organisatie sneller wil gaan, zullen er mogelijk extra maatregelen genomen moeten worden die die versnelling faciliteren. Dat kan extra mensen betreffen, verhoogde prioriteiten ten opzichte van andere veranderingen in de organisatie of het door andere organisaties laten uitvoeren van (delen van) het proces.
Wanneer de organisatie langzamer wil gaan, zal er waarschijnlijk een risico-inschatting gemaakt moeten worden van de consequenties voor de informatieveiligheid en het niet voldoen aan wet- en regelgeving. Die consequenties dienen dan wel door een verantwoordelijke gedragen te worden.

5 Overzicht capability-niveaus

Beveiligingsincident-management & response gaat over het vermogen, de processen, tools en technologieën van een organisatie voor het reageren op cyberdreigingen, cyberincidenten of cyberaanvallen. Met het assessment in dit document wordt gemeten in welke mate een organisatie over de vaardigheid beschikt die hier invulling aan geven.

Het assessment in dit document hanteert een viertal niveaus van capability. De capability-niveaus worden bepaald door de kenmerken die per niveau aan de beveiligingsincident-management & responseprocessen zijn toegewezen.

Hierna geven wij aan wat wordt verwacht voor de verschillende niveaus die gebruikt zijn om de capability-niveaus vorm te geven. Deze zijn ook weergegeven in Tabel 1 Capability-niveaus matrix. Wanneer een capability op beveliingsincidentmanagement & response nog niet verwacht wordt binnen een niveau is die op dat niveau ook niet beschreven. In de vragenlijst is wel nog steeds aangeven wat wij aan inrichting verwachten aan te treffen aan capabilities op incidentmanagement zonder expliciete aandacht voor informatiebeveiligingsincidenten.

5.1 Niveau 0

Beleid

Digitale weerbaarheid is geen structureel onderwerp van gesprek bij het senior management van de organisatie maar er is wel beleid voor (gewoon) incidentmanagement gedefinieerd.

Proces

Een organisatie beschikt over een meldpunt voor beveiligingsincidenten [BIO 16.1.2.1] en is in staat om te reageren op beveiligingsincidenten. Ook biedt de organisatie de mogelijkheid aan mensen van zowel binnen als buiten de organisatie om gevonden kwetsbaarheden te melden [BIO 6.1.3.1]. De procedures om beveiligingsincidenten te melden zijn gecommuniceerd naar medewerkers, aannemers, dienstverleners en andere belanghebbenden.

De organisatie maakt weinig tot geen onderscheid tussen beveiligingsincidenten en andersoortige incidenten. Het afhandelen van beveiligingsincidenten vindt op gelijksoortige manier plaats als voor reguliere incidenten. Ernstige beveiligingsincidenten worden gemeld bij relevante stakeholders en het CSIRT [BIO 16.1.4.1]. De opvolging van beveiligingsincidenten wordt bewaakt en er wordt over gerapporteerd [BIO 16.1.2.6].

Meldbronnen

Er is nog geen monitoring ingericht en incidenten komen door meldingen van gebruikers en andere betrokkene in het Incidentmanagement & -responseproces.

Responseplannen

Er zijn weinig of geen responseplannen uitgewerkt die handelingsperspectief op beveiligingsincidenten op voorhand beschrijven.

Responsebereik

De response is primair gericht op de eigen IT-systemen.

5.2 Niveau 1

Beleid

Het senior management van de organisatie heeft aandacht voor digitale weerbaarheid, maar deze aandacht is nog voornamelijk op ad-hoc basis. Er is beleid voor incident response vastgesteld [BIO 16.1.1] en dit beleid is afgestemd op de doelstellingen van de organisatie. Zowel lijnmanagement als senior management ontvangt periodiek rapportages over informatiebeveiligingenincidenten [BIO 16.1.2].

Proces

De organisatie beschikt over een meldpunt voor beveiligingsincidenten [BIO 16.1.2.1] en is in staat om gestructureerd te reageren op beveiligingsincidenten. Op niveau 1 beschikken organisaties over een procesgerichte aanpak voor beveiligingsincidenten en zijn de taken en verantwoordelijkheden van het meldpunt vastgelegd [BIO 16.1.2.2]. Voor de prioritering van beveiligingsincidenten wordt niet alleen naar de impact op de beschikbaarheid van IT-systemen gekeken, maar ook naar de potentiële dreiging die van de kwetsbaarheid en de exploitatie hiervan uitgaan. De organisatie heeft een meldpunt waar personen van zowel binnen als buiten de organisatie gevonden kwetsbaarheden kunnen melden [BIO 6.1.3.1]. De beveiligingsincident-management en -responseprocessen zijn beschreven waarbij proceseigenaren verantwoordelijk zijn voor het oplossen van incidenten [BIO 16.1.2]. Medewerkers, aannemers, dienstverleners en andere belanghebbende zijn aantoonbaar op de hoogte van de meldprocedure [BIO 6.1.2.3]. Ernstige beveiligingsincidenten worden gemeld bij relevante stakeholders en het CSIRT [BIO 16.1.4.1]. De opvolging van beveiligingsincidenten wordt bewaakt en gerapporteerd [BIO 16.1.2.6].

Rollen

Een organisatie op niveau 1 heeft, afhankelijk van de omvang, één of meerdere medewerkers die verantwoordelijk zijn voor informatiebeveiliging. Deze medewerker(s) ontvangen rapportages die inzicht geven in de beveiligingsincidenten die hebben plaatsgevonden [BIO 6.1.1].

Meldbronnen

Organisaties op niveau 1 hebben vormen van geautomatiseerde monitoring gerealiseerd zodat ze niet enkel op basis van verstoringen en externe meldingen afhankelijk zijn. De monitoring is nog niet centraal georganiseerd.

Responseplannen

Er is één generiek responseplan waarin ten minste de escalatie naar crisismanagement en dienstenleveranciers en de communicatie naar het CSIRT is beschreven.

Responsebereik

Het responseplan gaat over de eigen IT-systemen en de relatie naar de bedrijfseigenaren die van deze IT-systemen gebruik maken.

Testen & Oefeningen

Het responseplan is wel in opzet getest maar er wordt nog niet geoefend.

Evaluatie

Na een beveiligingsincident wat tot een crisis leidt, wordt een evaluatie gedaan wat kan leiden tot een aanpassing van het proces of het generieke responseplan.

5.3 Niveau 2

BIO Compliance

Dit niveau omvat organisaties waarvan verwacht mag worden dat deze, voor wat betreft incidentmanagement, compliant zijn aan de BIO. Ook wordt verwacht dat er risicomanagement, Business Continuity Management en leveranciersmanagement is ingericht omdat hierna verwezen wordt of gebruik van gemaakt wordt.

Beleid

Voor het senior management van de organisatie is digitale weerbaarheid een structureel agendapunt en er is aandacht voor dreigingen. Er is beleid voor incident response vastgesteld [BIO 16.1.1] en dit beleid is afgestemd op de doelstellingen van de organisatie. Het beleid wordt periodiek geëvalueerd en zo nodig bijgesteld [BIO 5.1.2.1].
Zowel het senior- als lijnmanagement ontvangt periodiek rapportages over informatiebeveiligings-incidenten en stuurt op basis daarvan bij [BIO 16.1.2].

Proces

De organisatie beschikt over een meldpunt voor beveiligingsincidenten [BIO 16.1.2.1] en is in staat om adequaat te reageren op beveiligingsincidenten. Er is een normenkader dat gebruikt wordt om incidenten als te classificeren [BIO16.1.3]. Het melden van incidenten gebeurt zo snel mogelijk en uiterlijk binnen 24 uur na bekend worden [BIO16.1.2.4]. Op niveau 2 beschikken organisaties over een gerichte aanpak voor beveiligingsincidenten en zijn zowel het proces alsmede de taken en verantwoordelijkheden van het meldpunt vastgelegd [BIO 16.1.2.2]. Verder zijn proceseigenaren en actoren getraind. De preparatie van incident responseplannen en de specifieke responseonderdelen zoals de containment en de relatie naar crisismanagement en naar recoverymanagement zijn beschreven als onderdeel van het proces. Voor de prioritering van beveiligingsincidenten wordt niet alleen naar directe operationele beschikbaarheid van IT-systemen gekeken, maar ook naar de potentiële impact die van de dreiging en de kwetsbaarheid uitgaan.

Rollen

De organisatie beschikt over een meldpunt waar personen van zowel binnen als buiten de organisatie gevonden kwetsbaarheden kunnen melden [BIO 6.1.3.1]. De incidentmanagement & responseprocessen zijn beschreven waarbij proceseigenaren verantwoordelijk zijn voor het oplossen van incidenten [BIO 16.1.2.5]. Medewerkers, aannemers, dienstverleners en andere belanghebbende zijn aantoonbaar op de hoogte van de meldprocedure [BIO 6.1.2.3].
De organisatie heeft, afhankelijk van de omvang, één of meerdere medewerkers in verschillende rollen die verantwoordelijk zijn voor informatiebeveiliging. Deze medewerker(s) ontvangen rapportages die inzicht geven in de beveiligingsincidenten die hebben plaatsgevonden. [BIO 6.1.1]

Meldbronnen

Een organisatie op dit niveau maakt gebruik van centrale en gecoördineerde beveiligingsmonitoring waarbij, naast externe meldingen, detectiesignalen als trigger dienen om het incident responseproces op te starten [BIO 6.1.2.1].

Responseplannen

Er zijn gedocumenteerde responseplannen voor en [BIO 16.1.5]. Kennis en best practices opgedaan bij het afhandelen van en worden gebruikt om de responseplannen te actualiseren [BIO16.1.6] en waar nodig wordt kennis met andere belanghebbenden gedeeld [BIO-16.1.6.2].
Ten minste voor Ransomware, Malware en Datalekken beveiligingsincidenten zijn uitgewerkte responseplannen beschikbaar. De responseplannen worden ieder jaar bijgewerkt.

Responsebereik
Organisaties op niveau 2 hebben de informatieketens in beeld en informatiebeveiliging is een integraal onderdeel van leveranciers- en klantenmanagement. Binnen de organisatie zijn lijnmanagers verantwoordelijk voor ketens van informatiesystemen [BIO 5.1.1.1.c]. Verder is er contact met relevante overheidsinstanties [BIO 6.1.3].

Testen & Oefeningen
De organisatie voert periodiek testen (self-assessments, table-top, audits, walk-throughs) uit die aantonen dat de processen response om te reageren op beveiligingsincidenten naar behoren functioneren.

Evaluatie
Voor hoge prioriteit beveiligingsincidenten wordt na afloop van het incident een evaluatie gemaakt die kan leiden tot een aanpassing van het proces en van de responseplannen.

5.4 Niveau 3
BIO Compliance
Dit niveau betreft organisaties welke wat betreft incidentmanagement en de aan digitale weerbaarheid verbonden processen zoals continuïteitsmanagement en leveranciersmanagement, compliant zijn aan de BIO.

Beleid
Binnen het senior management van de organisatie is digitale weerbaarheid een structureel agendapunt en er is aandacht voor dreigingen. Er is beleid voor Incident Response vastgesteld [BIO 16.1.1] en dit beleid is afgestemd op de doelstellingen van de organisatie. Het beleid wordt periodiek geëvalueerd en zo nodig bijgesteld [BIO 5.1.2.1]. Zowel het senior- als lijnmanagement ontvangt periodiek rapportages over informatiebeveiligingenincidenten [BIO 16.1.2]. Daarnaast wordt er gerapporteerd over zwakke plekken in de informatiebeveiliging [BIO-16.1.3, BIO-16.1.2.7].

Proces
De organisatie beschikt over een meldpunt voor beveiligingsincidenten [BIO 16.1.2.1] en is in staat om te reageren op beveiligingsincidenten. Er is een normenkader dat gebruikt wordt om incidenten als beveiligingsincidenten te classificeren [BIO16.1.3]. Het melden van incidenten gebeurt zo snel mogelijk en uiterlijk binnen 24 uur na bekend worden [BIO16.1.2.4]. Op niveau 3 beschikken organisaties over een gerichte aanpak voor beveiligingsincidenten en is zowel met proces alsmede de taken en verantwoordelijkheden van het meldpunt vastgelegd [BIO 16.1.2.2]. Verder zijn proceseigenaren en actoren getraind. Voor de prioritering van beveiligingsincidenten wordt niet alleen naar directe operationele beschikbaarheid van IT-systemen gekeken, maar ook naar de potentiële impact op de (kritische) processen binnen de organisatie die van de dreiging en de kwetsbaarheid uitgaan. De organisatie beschikt over een meldpunt waar personen van zowel binnen als buiten de organisatie gevonden kwetsbaarheden kunnen melden [BIO 6.1.3.1]. Er is integratie tussen de monitoringprocessen en de monitoringsystemen aan de voorkant van het proces voor de incident afhandeling. Er is integratie tussen de response-afhandeling en bedrijfscontinuïteitmanagement waaronder crisismanagement en recoverymanagement aan de achterkant van het proces. Er is integratie met de informatiebeveiliging en de risicobeoordeling binnen de organisatie voor de classificering en prioritering van de beveiligingsincidenten.

Rollen
De organisatie heeft, afhankelijk van de omvang, één of meerdere medewerkers die verantwoordelijk zijn voor informatiebeveiliging. Deze medewerker(s) ontvangen rapportages die inzicht geven in de beveiligingsincidenten & response die hebben plaatsgevonden. [BIO 6.1.1]

De beveiligingsincident-management & response processen zijn beschreven waarbij proceseigenaren verantwoordelijk zijn voor het oplossen van incidenten [BIO 16.1.2]. Medewerkers, aannemers, dienstverleners en andere belanghebbende zijn aantoonbaar op de hoogte van de meldprocedure [BIO 6.1.2.3].

Meldbronnen

De organisatie beschikt over een volwassen SOC met ruime ervaring dat zich heeft gevormd tot een Cyber Defense Center. Een Cyber Defense Center is een combinatie van een SOC en een CSIRT (Computer Security Incident Response Team) die delen van het beveiligingsincident-management & response kan overnemen van de organisatie. Hierdoor is de organisatie in staat de meldingen voor het grootste gedeelte automatisch te genereren. Het Cyber Defense Center is in staat om (potentiële) beveiligingsincidenten te signaleren en vervolgens adequaat te voorzien in Incident Response [BIO 6.1.2.1].

Responseplannen

Er zijn gedocumenteerde procedures voor response op en [BIO 16.1.5]. Organisaties op niveau 3 beschikken over procedures voor het identificeren, verzamelen, verkrijgen en bewaren van bewijsmateriaal [BIO-16.1.7]

Naast uitgewerkte responseplannen voor Ransomware, Malware en Datalekken heeft de organisatie een uitgebreidere set responseplannen beschikbaar die zijn samengesteld op basis van een organisatie specifieke dreigingsanalyse. De responseplannen worden gedreven vanuit de impact op de meest kritische bedrijfsprocessen en worden jaarlijks herzien.

Responsebereik

Organisaties op niveau 3 hebben de informatieketens in beeld en informatiebeveiliging is een integraal onderdeel van leveranciersmanagement. Binnen de organisatie zijn lijnmanagers verantwoordelijk voor ketens van informatiesystemen [BIO 5.1.1.1.c].

Testen en Oefeningen

De organisatie voert periodiek testen uit die meten dat beveiligingsincident-management & response voldoet aan gestelde Kritieke Proces Indicatoren (KPI's). Daarnaast laat de organisatie periodiek door onafhankelijke externe partijen Red Teaming, of TIBER[1], testen uitvoeren en implementeert op basis van (relevante) bevindingen maatregelen in de responseplannen [BIO 18.2.3].

Tenminste jaarlijks vinden er realistische oefeningen plaats waarbij alle belanghebbenden in het ecosysteem meedoen.

Evaluatie

Er vinden evaluaties plaats van alle beveiligingsincidenten en de organisatie kenmerkt zich als een lerende weerbare organisatie [BIO 16.1.6]. Waar nodig wordt kennis met andere belanghebbende gedeeld [BIO 16.1.6.2].

[1] TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Het betreft uitgebreide testen welke voornamelijk geschikt zijn voor volwassen organisaties.

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