GENERIEK INCIDENT RESPONSE PLAN VOOR SOC OMGEVINGEN

DEEL B

Incident Management – Incident Response

Template versie 1.1

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord 3
Achtergrond 3
Doelgroep 3

1 Documentgegevens 4
1.1 Eigenaarschap 4
1.2 Documenthistorie 4
1.3 Distributielijst 4
1.4 Referenties 4
2 Inleiding 5
2.1 Context 5
2.2 Doel & Doelstellingen 5
2.3 Scope 5
2.4 Leeswijzer 5
3 Draaiboek 6
3.1 Incident Response Scope 6
3.2 Registratie & Verificatie van meldingen 7
3.3 Classificatie & Prioriteren 7
3.4 Onderzoek & diagnose, Beheersen, Oplossen & herstellen 8
3.5 Post-incident activiteiten 10

Bijlage I: Checklist voorbereiding 11
Bijlage II: Incident Meldingsformulier 13
Bijlage III: Incident Triage 15
Bijlage IV: Template Playbook 16
Bijlage V: Lessons learned 19

Voorwoord

Digitale weerbaarheid is een randvoorwaarde voor het goed functioneren van iedere organisatie binnen de overheid. Incidenten in de informatievoorziening kunnen niet alleen de continuïteit van onze dienstverlening raken, maar ook het vertrouwen van burgers, partners en medewerkers.

Het Cyber Incident Response Plan (CIRP) bestaat uit 2 delen. In deel A legt de organisatie de juiste inrichting vast. Het beschrijft hoog over hoe in de organisatie gecoördineerd, transparant en doeltreffend moet worden gehandeld bij cyber security incidenten en wie daarin welke rol heeft. Het plan biedt een uniform raamwerk dat vooral bij de voorbereiding op een cyber incident zijn meerwaarde heeft. Het document dat u voor zicht heeft is deel B. Deel B van het CIRP biedt vooral een praktisch handvat dat tijdens een cyber incident erbij kan worden gepakt en de betrokkenen begeleidt bij de te nemen acties. Beide documenten (zowel A als B) dienen op basis van organisatie-specifieke kenmerken, wensen en eisen nog wel uniek te worden gemaakt. Beiden documenten samen vormen het volledige CIRP.

Het Incident Response Plan is bedoeld als praktisch instrument: een leidraad voor iedereen die betrokken is bij de digitale beveiliging en crisisbeheersing. Door cyber incident respons met behulp van het CIRP regelmatig te oefenen, te evalueren en te verbeteren, wordt de weerbaarheid vergroot. Waar nodig dient het CIRP n.a.v. evaluatiepunten uit de oefeningen (of incidenten) te worden aangepast.

Dit document is tot stand gekomen in een samenwerkingsverband tussen het Security Operations Center (SOC) van het Ministerie van Justitie en Veiligheid, Nederlands Instituut Publieke Veiligheid (NIPV) en Versterken SOC Stelsel Rijk (VSSR) wat onderdeel uitmaakt van het Nationaal Cyber Security Centrum (NCSC).

Achtergrond

Elke organisatie doet er goed aan te beschikken over een Cyber Incident Response Plan (CIRP). Het CIRP is bedoeld als praktisch instrument om de digitale weerbaarheid van uw organisatie te verbeteren.

Doelgroep

Dit document beoogt een handvat te bieden voor iedereen die binnen elke organisatie betrokken is bij digitale beveiliging, incident respons en crisisbeheersing.

1 Documentgegevens

Dit Cyber Incident Response Plan (CIRP) is een levend document dat eigendom is van de *[Rol]* van de organisatie.

[Rol] is verantwoordelijk voor het onderhoud, de actualiteit en de verspreiding van dit document. Benodigde aanpassingen worden in ieder geval jaarlijks geëvalueerd en vastgelegd in onderstaande wijzigingshistorie.

De actuele distributielijst van functionarissen en afdelingen die toegang hebben tot het IRP wordt beheerd door [Rol] en is hieronder opgenomen. Alleen geautoriseerde medewerkers mogen wijzigingen aanbrengen of goedkeuren.

1.1 Eigenaarschap

Document	Link
Auteur	
Eigenaar	
Datum gecreëerd	
Gereviewd door	
Review datum	
Goedgekeurd op	

1.2 Documenthistorie

Versie	Datum	Omschrijving
V1.0	5-3-2026	Initiële versie
V1.1	2-7-2026	Referenties geactualiseerd

1.3 Distributielijst

Versie	Datum	Gedistribueerd naar
V1.0	06-03-2026	*CIO, CISO, SOC, etc.*

1.4 Referenties

Document	Link
VSSR CIRP Deel A	Cyber Incident Response Plan - Deel A - Draaiboek
Incident Response draaiboeken (VSSR)	Draaiboeken/Playbooks
Incident Response kennisproducten van VSSR	Incident Response Readiness
Kroonjuwelenoverzicht	Assetmanagement - Overzicht Kroonjuwelen
Netwerkoverzicht	Netwerkmanagement - IP Nummerplan
Accountoverzicht	Identitymanagement - Accountoverzicht

2 Inleiding

Dit document is het draaiboek voor de organisatie te gebruiken bij Cyber Security gerelateerde incidenten. Het beschrijft wat, wanneer en hoe moet worden ondernomen voor verschillende type cyber incidenten. Per type incident is een afzonderlijk draaiboek beschikbaar gesteld wat ingaat op specifieke handelingen van toepassing voor dat type incident.

2.1 Context

Binnen de organisatie bestaan er een aantal kritische processen. Deze processen moeten altijd door blijven gaan, of moeten bij onderbreking weer zo snel mogelijk operationeel worden gebracht. Het Cyber Dreigingslandschap is als maar groeiend en veranderend en de organisatie is ook meer en meer onderhevig aan verschillende soorten van aanvallen met variërende implicaties. Om verschillende dreigingen en aanvallen het hoofd te kunnen bieden, moet de organisatie goed voorbereid zijn en snel kunnen schakelen in geval van nood. Dit draaiboek biedt de handvatten om bij verschillende aanvallen op de juiste manier te reageren zodat de potentiële schade bij een incident zoveel mogelijk kan worden beperkt en kritische processen zo min mogelijk direct worden beïnvloed.

2.2 Doel & Doelstellingen

Doel: Dit document beschrijft het algemene draaiboek voor Cybersecurity Incidenten en bevat alle noodzakelijke elementen om in geval van een incident snel en adequaat te kunnen reageren.

Doelstellingen:

1. Inzicht bieden in de scope van het incident response proces;
2. Duiden wat een incident precies is, hoe deze in te schalen en hoe te reageren per incident type/ernst;
3. Bieden van eenduidig handelsperspectief bij incidenten;
4. Vastleggen van escalatiepaden;
5. Vastleggen van een volledige en correcte lijst van contactpersonen.

2.3 Scope

Incident Response is een belangrijk onderdeel binnen een breed scala aan onderwerpen binnen informatiebeveiliging. Om te zorgen dat de organisatie op alle fronten de juiste zeken doet, wordt het NIST CSF (2.0) gebruikt als referentiekader voor een omvangrijkere strategie. Binnen dit referentiekader komen de onderwerpen: Besturen, Herkennen, Beschermen, Detecteren, Reageren, en Herstellen aan bod. De scope van dit document betreft alleen het Reageren op cyber incidenten en beschrijft wat moet worden gedaan en hoe moet worden gehandeld voor verschillende incidenten.

2.4 Leeswijzer

Dit document beschrijft in detail hoe en wanneer gehandeld dient te worden bij de verschillende incidenten die binnen het incident response proces worden afgehandeld. Het draaiboek is heel beknopt en bevat verschillende bijlagen ter ondersteuning van de verschillende processtappen. De bijlagen kunnen los worden gebruikt of kunnen in het document worden geïntegreerd. Houd voor het hele document in het achterhoofd dat elke organisatie veel zal kunnen hergebruiken maar dat een deel ook altijd organisatiespecifiek is en dus naar eigen behoefte ingevuld dient te worden.

3 Draaiboek

Dit draaiboek beschrijft, voor de verschillende incidenttypes en ernst van het incident, welke acties ondernomen dienen te worden. Het draaiboek is generiek van aard en breed toepasbaar. Naast dit draaiboek wordt er gerefereerd naar incidenttype specifieke draaiboeken die voor dat type incident van toepassing zijn. Voor de incidenttypen waar geen afzonderlijk draaiboek van toepassing is, is dit draaiboek leidend.

Hierin wordt uitgegaan van de processtappen zoals uiteengezet in het standaard proces:

- Registratie & verificatie : Vastlegging en verificatie het (beveiligings-) incident
- Classificatie & prioriteren : Vaststellen prioriteit op basis van impact en urgentie
- Onderzoek & diagnose : Identificeren van het beveiligingsincident
- Containment : Impact beveiligingsincident beperken en te beheersen
- Oplossing & herstel : Toepassen permanente oplossingen en herstelmaatregelen
- Post-incident activiteiten : Optimaliseren incident responsestrategieën

3.1 Incident Response Scope

De scope waarop het incident response draaiboek van toepassing is, betreft in eerste instantie de belangrijkste Te Beschermen Belangen en de ondersteunende ICT-kroonjuwelen van de organisatie. Hieronder vallen:

- Kritische processen en procesketens en bijbehorende eigenaren;
- Ondersteunde diensten en bijbehorende applicaties;
- Bijbehorende ICT-assets;
- De belangrijke Network Segmenten waar deze assets zijn geplaatst;
- De Identities die toegang hebben tot deze assets; en,
- Gevoelige data met betrekking tot deze processen en diensten.

Hieronder zijn de kritische processen, in-scope voor dit document, opgenomen samen met eigenaarschap en ondersteunende applicaties. Verdere, veelal technische, details zijn in afzonderlijke documenten opgenomen (zie *1.3 Distributielijst*

Versie	Datum	Gedistribueerd naar
V1.0	06-03-2026	*CIO, CISO, SOC, etc.*

Referenties).

Versie	Datum	Gedistribueerd naar
V1.0	31-03-2026	*CIO, CISO, SOC, etc.*

3.1.1 Proces: <naam kritisch proces 1>

Proces: <TBD>
Eigenaar: <TBD>

Dienst	Applicaties	Afhankelijkheden

3.1.2 Proces: <naam kritisch proces 2>

Proces: <TBD>
Eigenaar: <TBD>

Dienst	Applicaties	Afhankelijkheden

3.2 Registratie & Verificatie van meldingen

Potentiële incidenten kunnen op verschillende manier worden geïdentificeerd:

1. Externe melding: Een externe partij kan een kwetsbaarheid of mogelijk incident aanmelden, bijvoorbeeld via een daarvoor beschikbaar gestelde website (volgens template: *Bijlage II: Incident Meldingsformulier*), maar bijvoorbeeld ook telefonisch of via email via de contactinformatie beschikbaar gesteld op de website als genoemd in CIRP document Deel A;
2. Detectie: Incidenten kunnen worden gemeld door het (in- of extern) Security Operations Center (SOC) waar ongebruikelijke voorvallen worden gedetecteerd en onderzocht;
3. Interne Melding: Interne medewerkers kunnen (potentiële) incidenten melden via de service desk of direct bij het SOC;
4. Melding vanuit leveranciers: Dienst- of productleveranciers kunnen melding maken van relevante incidenten die zich bij hun voordoen en die mogelijk van impact zijn op de organisatie of van mogelijke incidenten binnen de eigen organisatie maar opgemerkt door de leverancier.

Alle meldingen worden vastgelegd in het incident management systeem en volgens procedure opgevolgd.

Acties

- Verifieer de registratie van het voorval of registreer het zelf;
- Verifieer de informatie die is opgenomen tijdens de registratie en corrigeer waar nodig;
- Volg de algemene triage stappen zoals beschreven in *Bijlage III: Incident Triage*;
- Leg de bevindingen vast in het incident management systeem volgens de bijgevoegde template: *Bijlage II: Incident Meldingsformulier*.

3.3 Classificatie & Prioriteren

De organisatie onderkent verschillende typen incidenten en daarbij verschillende niveaus van ernst. Voor het categoriseren en classificeren, zijn onderstaande tabellen voorschrijvend.

De “Algehele Incident Classificatie & Prioritering" (zie Deel A) geldt als algemene leidraad voor het inschalen van incidenten waar de tabel met “Specifieke Incident Categorisatie & Prioritering” een verbijzondering is voor specifieke incidentcategorieën waarbij de Ernst-bepaling als eerste en minimale indicatie geldt maar mogelijk naar boven bijgesteld moet worden afhankelijk van de situatie.

Acties

- Voer classificatie en prioritering uit volgens onderstaande tabellen;
- Communiceer het incident naar de juiste oplospartij. Dit kan een externe leverancier zijn, een applicatie of proceseigenaar, maar ook een incident responder die eerst verder/diepgaander onderzoek zal uitvoeren naar het incident en volgens het juiste draaiboek verdere opvolging zal verzorgen.

Specifieke Incident Categorisatie & Prioritering

Type	Ernst	Beschrijving
Denial of Service	Hoog	Type aanval waarbij een Dienst onbeschikbaar wordt gemaakt door een aanvaller veelal (maar niet alleen) door het overweldigen van de dienstverleningsomgeving met bovenmatige hoeveelheden data.
Ransomeware	Kritiek	Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld of om deze data te gebruiken voor chantage anderszins.
Phishing	Midden	Phishing is een aanvalstechniek die wordt ingezet om gevoelige informatie te ontfutselen (die eventueel later voor andere doeleinden, zoals inbraak, kan worden ingezet) of om direct in te breken bij de organisatie. De meest gangbare vorm gebeurt via email, maar dit is zeker niet de enige methode.
Malware uitbraak	Midden	Aanval waarbij Malafide software wordt gebruikt die zichzelf in hoog tempo door de organisatie verspreid en voor grootschalige verstoring zorgt.
Data Breach	Kritiek/Hoog	Aanval waarbij gevoelige informatie (voor de organisatie of van klanten) wordt gestolen.
Public Service Breach	Hoog	Aanval waarbij een publieke dienst wordt gecompromitteerd met als gevolg onbeschikbaarheid of reputatieschade. Onbeschikbaarheid kan, afhankelijk van de criticaliteit van de dienst, in alternatieve inschaling resulteren.
Supply Chain Attack	Midden	Bij dit type aanval wordt voornamelijk gerefereerd aan software compromittering door het gebruik van bibliotheekcomponenten of modules van externe leveranciers waar een aanvaller moedwillig malafide code op heeft geïntroduceerd. Dit kan grootschalige impact hebben op ontwikkelstraten en uitgerolde componenten in productie-omgevingen.
Verder aanvullen		*Vul deze lijst verder aan op basis van een organisatie-specifieke dreigingsanalyse die laat zien wat voor de organisatie de belangrijkste aanvallen kunnen zijn. Zo kan bijvoorbeeld voor een organisatie die veel gebruik maakt van IoT of OT componenten een aanval op deze infrastructuur van essentieel belang zijn.*

3.4 Onderzoek & diagnose, Beheersen, Oplossen & herstellen

Verschillende typen incidenten vereisen een verschillende aanpak. Binnen de organisatie is per incidenttype een afzonderlijk draaiboek vastgesteld die de stappen voor *Onderzoek, Beheersing en Oplossen* bevat.

Acties

- Gebruik onderstaande tabel voor het identificeren van het juiste draaiboek;
- Volg het draaiboek voor het specifieke incident;
- Gebruik de verdere sub-paragrafen in deze sectie voor hun specifieke doeleinden als mogelijke verbijzondering of aanvulling op het draaiboek.

3.4.1 Ondersteunende incidentdraaiboeken

Een incidentdraaiboek is een stap-voor-stap handboek dat wordt doorlopen bij incidenten om de juiste acties uit te voeren. Per incidenttype is een specifiek draaiboek beschikbaar. De draaiboeken zijn opgesteld volgens de template in *Bijlage IV: Template Playbook* met verbijzondering waar nodig.

Hieronder is een lijst met beschikbare draaiboeken opgenomen met een link naar de locatie waar deze is opgeslagen.

Type	Aanwezig	Locatie
Internet Facing kritische Kwetsbaarheid	Ja	Draaiboek: Internet facing kritische kwetsbaarheid
Supply Chain Aanval	Ja	Draaiboek: Supply Chain Attack
Denial of Service	Ja	*[Link]*
Ransomeware	Ja	*[Link]*
Datalek	Ja	*[Link]*
Phishing	Nee	*[Link]*
Malware uitbraak	Nee	*[Link]*
Internet Service Compromittering	Nee	*[Link]*

3.4.2 Beheersings- en Besluitenmatrix

Hieronder is aangegeven, per type incident, welke beheersingsmaatregelen in geval van nood moeten worden toegepast en wie de mandaathouder is. Deze maatregelen komen ook voor de in de draaiboeken maar zijn mogelijk niet altijd nodig. De draaiboeken geven in meer detail aan wanneer het moet gebeuren, hieronder ligt de nadruk op de mandaathouder.

Ernst	Beheersingsmaatregel	Mandaathouder
Kritiek	Onmiddellijke isolatie	Houder stekkermandaat
Hoog	Gecontroleerde isolatie	CISO/SOC-Manager/Eigenaar
Gemiddeld	Monitoring + beperkte maatregelen	SOC-Manager
Laag	Verhoogde logging	SOC-Lead
Informatief	Niet van toepassing	Niet van toepassing

3.4.3 Contactgegevens

In onderstaande tabel zijn de verschillende contactgegevens opgenomen die per incidentniveau/rol kunnen worden aangewend waar van toepassing.

Niveau	Rol / functie	Contactgegevens
Decentraal	CISO	[invullen]
Departementaal	CISO	[invullen]
Nationaal	NCSC (ernstig incident, Wbni)	[invullen]
Nationaal	NCTV/NCC (digitale crisis)	[invullen]
Extern	Autoriteit Persoonsgegevens (datalekken)	[invullen]

3.5 Post-incident activiteiten

Dit laatste onderdeel van de incidentafhandeling is tweeledig. Ten eerste is het een finale afronding en daarnaast is het bedoeld om te leren van eerdere incidenten om het proces te verbeteren.

Bij de afronding van het lopend incident zijn een aantal zaken van belang:

- Meld het incident af en praat alle stakeholders bij;
- Maak een goede Root-cause analysis waarbij gebruik kan worden gemaakt van de bijgevoegde template: *Bijlage V: Lessons learned;*
- Zorg dat tijdig aan alle rapportage verplichtingen wordt voldaan (zoals richting het NCSC).

Als aan alle verplichtingen is voldaan, is het tijd om het incident en vooral de afhandeling verder te evalueren. Gebruik de evaluatie voor procesverbeteringen en het aanscherpen van documentatie. Voor de verdere evaluatie kan ook weer de bijgevoegde template worden gebruikt: *Bijlage V: Lessons learned.*

Bijlage I: Checklist voorbereiding

Voorbereiding

- ☐ Incident response team getraind en beschikbaar
- ☐ Contactlijsten actueel
- ☐ Scoping, infrastructuur en assets bekend
- ☐ Response tools operationeel (SIEM, forensics, communicatie)
- ☐ Playbooks voor veelvoorkomende scenario's beschikbaar
- ☐ Juridische en regulatoire vereisten gedocumenteerd
- ☐ Backup en herstel procedures getest
- ☐ Communicatie sjablonen voorbereid
- ☐ Escalatie procedures gedefinieerd
- ☐ Forensische dienst (in- of extern) inzetbaar
- ☐ Beveiligde communicatiekanalen getest

Registratie & Verificatie

- ☐ Event is geregistreerd
- ☐ Event is geverifieerd
- ☐ Event is bekeken en toegewezen aan een analist
- ☐ Informatie in de registratie is gecontroleerd en aangevuld
- ☐ Getroffen systemen/gebruikers geïdentificeerd
- ☐ Event triage is uitgevoerd
- ☐ Bevindingen zijn vastgelegd

Classificatie & Prioriteren

- ☐ Event is gecategoriseerd volgens de categorisatiematrix
- ☐ Event is geclassificeerd volgens ernst matrix
- ☐ Vastgesteld of het event een potentieel incident betreft
- ☐ Potentiële impact is bepaald op basis van de impact categorieën
- ☐ Alle relevante informatie is vastgelegd volgens standaard incident rapport template
- ☐ Incident is doorgezet naar de juiste analist/incident handler/eigenaar (incident rapportage)

Onderzoek & Diagnose

- ☐ Attack vector bepaald
- ☐ Tijdlijn van compromis vastgesteld
- ☐ Potentiële data impact beoordeeld
- ☐ Stakeholders geïnformeerd
- ☐ Bewijs veiliggesteld

Beheersing

- ☐ Initieel beheersingsplan opgesteld
- ☐ Getroffen systemen geïsoleerd
- ☐ Gecompromitteerde accounts uitgeschakeld
- ☐ Kwaadaardige activiteit gestopt
- ☐ Verdere verspreiding voorkomen
- ☐ Business impact geminimaliseerd
- ☐ Monitoring uitgebreid
- ☐ Documentatie bijgewerkt

Oplossen & Herstel

- Malware verwijderd
- Kwetsbaarheden gepatcht
- Toegangscontroles bijgewerkt
- Monitoring geïmplementeerd
- Backups geverifieerd als schoon
- Services operationeel
- Prestaties acceptabel
- Beveiligingsmaatregelen functioneel
- Gebruikers kunnen veilig werken
- Compliance vereisten nageleefd

Post-incident activiteiten

Onmiddellijke Post-Incident (24-48 uur):

- Incident documentatie voltooid
- Bewijs veiliggesteld
- Stakeholder-briefing uitgevoerd
- Threat intelligence bijgewerkt
- Response effectiviteit analyse uitgevoerd
- Lessons-learned vastgesteld
- Procesverbeteringen geïdentificeerd en doorgevoerd
- Draaiboeken bijgewerkt

Bijlage II: Incident Meldingsformulier

Gegevens van melder	
Naam melder	:
Organisatie	:
Email adres	:
Telefoonnummer	:
Relatie (klant, leverancier, …)	:

Datum & tijd van het incident	
Start van het incident	:
Ontdekking van het incident	:
Beëindiging incident	:

Beschrijving van het incident	
Gedetailleerde beschrijving	:
Wat is er gebeurd	:
Wie of wat is er betrokken	:
Waar heeft het incident plaatsgevonden (fysiek of digitaal)	:

Type incident	
Phishing of spoofing	☐
Datalek / ongeautoriseerde toegang tot personeelsgegevens	☐
Malware / ransomeware	☐
Ongeautoriseerde toegang tot ruimtes of systemen	☐
Verlies of diefstal van hardware of documenten	☐
Social engineering	☐
Verstoring dienstverlening (DoS of DDoS)	☐
Overige (toelichting)	:

Betrokken systemen of gegevens	
Welke systemen, applicaties of platforms zijn betrokken	:
Zijn er persoonsgegevens betrokken?	☐
- Zo ja, hoeveel?	:
Zijn er vertrouwelijke bedrijfsgegevens betrokken?	:

Maatregelen die al zijn genomen	
Is er al ergens anders melding gedaan?	:
Zijn er systemen afgesloten of geïsoleerd?	:
Zijn er wachtwoorden gewijzigd?	
Is er al een technisch onderzoek gestart?	

Urgentie-inschatting door melder	
Hoe ernstig schat u het incident in? *(Laag / Midden / Hoog / Kritiek)*	:
Motivatie voor deze inschatting	:

Mogelijkheid voor toevoegen bijlagen / bewijsstukken	
Screenshot	:
Emails	:
Logs	:
Rapportage	:
Overig	:

Toestemming en verwerking	
Verklaring dat het formulier naar waarheid is ingevuld	☐
Toestemming voor verwerking van persoonsgegevens	☐
Verklaring dat er contact opgenomen kan worden met de melder	☐

Bijlage III: Incident Triage

Bij het analyseren van een event/incident is het van belang om zoveel mogelijk vragen te stellen. Hou hierbij het **Analyse Raamwerk** in het achterhoofd. De **Analyse Checklist** zijn zaken die bij de triage altijd aan bod moeten komen, maar het is zeker geen uitputtende (eerder een minimale) lijst met checks voor het afronden van de analyse.

Analyse Raamwerk:

WIE: Wie heeft de aanval uitgevoerd, is de Threat Actor te identificeren?
WAT: Wat was de aanvalsmethoden en, zo mogelijk, gebruikte payloads
WAAR: Waar vond de plaats, wat zijn de getroffen systemen en personen?
WAAROM: Waarom is het doelwit aangevallen (data, bestaande kwetsbaarheid, etc.)?
WANNEER: Kunnen de exacte tijdlijn van de aanval worden gereconstureerd?
HOE: Welke aanvalsvectoren en technieken zijn gebruikt en zijn deze vastgelegd.

Analyse Checklist:

- ☐ Type incident is bepaald (DDoS, Datalek, Phishing, etc.)
- ☐ Getroffen systemen/personen geïdentificeerd
- ☐ Incident geclassificeerd volgens ernst matrix
- ☐ Bepaald of het incident nog actueel is
- ☐ Attack vector bepaald
- ☐ Tijdlijn van de gebeurtenis is vastgesteld
- ☐ Potentiële (data) impact beoordeeld
- ☐ De aanval is bekeken binnen een bredere context van andere voorvallen en incidenten.

Bijlage IV: Template Playbook

Detectie & Analyse – Gedetailleerde Procedure
Doel: Bevestig [aanval]-activiteit, bepaal de omvang en beoordeel de impact.

Initiële Detectie

- Controleer SIEM/EDR-meldingen: Bijv. ongebruikelijke bestandshernoemingen, plotselinge CPU-pieken, losgeldberichten;
- Controleer e-mailbeveiligingsmeldingen op phishing;
- Start een incidentlogboek en ken een uniek incident-ID toe.

Incident Registratie

Registreer het incident in het ITSM-systeem of ticket registratiesysteem. Volg de stappen voor het invullen van de benodigde informatie.

In het geval dat er geen ITSM of ticket registratiesysteem aanwezig is gebruik het Bijlage II: Incident Meldingsformulier.

Analyse

In de analysefase word alle benodigde informatie verzameld en geanalyseerd, hierdoor ontstaat er een incidentfoto, hoe meer informatie beschikbaar en geanalyseerd hoe beter de foto.

Bewijsverzameling	
Maak forensische kopieën	☐ - Geheugen ☐ - VHD/VDMK/HDD/SSD ☐ - N.V.T.
Verzamel logs	☐ - Firewall ☐ - IDS/IPS ☐ - Proxy ☐ - NetFlow ☐ - Authenticatie LDAP/MS AD/MS AAD(EntraID) ☐ - Anders, namelijk: _____ _____ _____
Malware / ransomware	☐ Malware ☐ Ransomware

Omvang bepalen (scope)	
Initiele ingang (patient zero)	:
Heeft patient zero contact gehad met andere systemen?	☐ Nee ☐ Ja
Zijn er systemen afgesloten of geïsoleerd?	☐ Nee ☐ Ja
Zijn er wachtwoorden gewijzigd?	☐ Nee ☐ Ja
Is er al een technisch onderzoek gestart?	☐ Nee ☐ Ja
Inspecteer uitgaand netwerkverkeer op grote versleutelde overdrachten. (Ter controle op mogelijk gegevensdiefstal)	☐

Maak hashes en bewaar geëxfiltreerde bestanden voor AP/AVG-melding	☐ (Alleen van toepassing als het vermoeden is op gegevensdiefstal)

Controle op gegevensdiefstal	
Inspecteer uitgaand netwerkverkeer op grote versleutelde overdrachten.	☐
Controleer met DLP-tools of persoonsgegevens zijn geëxfiltreerd.	☐ (Alleen van toepassing als tools daadwerkelijk aanwezig zijn)
Maak hashes en bewaar geëxfiltreerde bestanden voor AP/AVG-melding	☐ (Alleen van toepassing als het vermoeden is op gegevensdiefstal)

Impact en escalatie

Nadat de analyse is gedaan moet er een impact beoordeling worden ondernomen en worden bepaald welke escalatie benodigd is.

Impact & Escalatie	
Beoordeel impact op vertrouwelijkheid, integriteit en beschikbaarheid.	☐
Incident met hoog impact?	☐ (Beoordeel op het interne escalatiemodel)
Escalatie nodig?	☐ Ja (Beoordeel op basis van interne escalatiemodel)

Incident bestrijding

Als eenmaal de impact analyse en escalatie uitgevoerd moet het incident zo snel mogelijk worden bestreden. Dit gebeurt door eerst het incident te isoleren (inperken). Wanneer het inperken is afgerond kan het verwijderen van de bestanden etc. Als laatste begint het herstellen van de operatie. Tijdens al deze stappen is juist communicatie enorm belangrijk, blijf deze stappen continue uitvoeren, het zijn ***geen*** eenmalige acties.

Inperking	
Koppel geïnfecteerde systemen los van het netwerk, maar laat ze ingeschakeld voor bewijsmateriaal.	☐
Schakel gecompromitteerde account(s) uit en dwing wachtwoord reset(s) af.	☐
Controleer recente privilege-escalaties.	☐
Blokkeer kwaadaardige IP's/domeinen en verdacht verkeer (bijv. SMB of RDP).	☐
Isoleer netwerken waar mogelijk	☐
Koppel back-upservers onmiddellijk los of unmount ze	☐
Controleer of back-ups niet versleuteld zijn	☐

Communicatie	
Gebruik veilige communicatiekanalen	☐ (Evt. buiten het eigen netwerk)
Informeer stakeholders	☐ (Op basis van escalatiemodel en contactpunten en meldstructuur)
Geef periodiek updates	☐ (Bijv. elk uur, of 3 maal per dag)

Meld bij de Autoriteit Persoonsgegevens binnen 72 uur als gegevens zijn getroffen.	☐ (Zorg voor het betrekken van de juiste rol (CPO/PO))
Informeer NCSC-NL en relevante sector-CERT.	☐
Meld het incident bij het Team High Tech Crime van de Politie.	☐
Bereid een persverklaring voor die het incident erkent zonder gevoelige details.	☐
Informeer medewerkers transparant.	☐
Deel geanonimiseerde IoC's en geleerde lessen met NCSC-NL en sectorpartners.	☐

Eradicatie & Herstel	
Verwijder (ransomware-)bestanden en persistentie-mechanismen	☐
Zoek naar en verwijder tools voor laterale beweging	☐
Patch misbruikte kwetsbaarheden en schakel onnodige diensten uit	☐
Update endpoint bescherming en SIEM-detectieregels.	☐
Scan back-ups offline om besmetting uit te sluiten.	☐
Herstel kritieke diensten eerst en monitor herstelde systemen.	☐
Reset alle bevoorrechte ((high)privileged) en serviceaccount-wachtwoorden.	☐
Heruitgifte van gecompromitteerde TLS/PKI-certificaten indien nodig.	☐

Bijlage V: Lessons learned

Introductie

Het doel van een lessons learned-document is het identificeren en begrijpen van de oorzaken van een incident, en het ontwikkelen van strategieën om vergelijkbare incidenten in de toekomst te voorkomen.

Het lessons learned-proces wordt gebruikt om waardevolle informatie en inzichten die tijdens een incident zijn opgedaan vast te leggen, en deze te benutten om de incidentrespons van de organisatie te verbeteren.

Dit kan onder meer inhouden:

- Het identificeren van lacunes of zwakke punten in het incidentresponsplan van de organisatie;
- Het doorvoeren van aanpassingen om deze problemen aan te pakken.

Een lessons learned-document kan ook helpen bij het aanwijzen van gebieden waar de incidentrespons verder kan worden verbeterd, en biedt richtlijnen en aanbevelingen voor toekomstige incidentresponsactiviteiten.

Uiteindelijk is het doel van een lessons learned-document in de context van incidentrespons om organisaties te helpen beter voorbereid te zijn op incidenten en de impact van toekomstige incidenten op de organisatie en haar stakeholders te minimaliseren.

Context

Beschrijf de context waarbinnen het incident heeft plaatsgevonden.

Inclusief:

- De specifieke systemen die erbij betrokken waren.
- De bedrijfsprocessen die door het incident zijn beïnvloed.
- De potentiële risico’s voor de organisatie.

Hierbij kan worden ingegaan op factoren zoals de operationele omgeving, de tijd en duur van het incident, relevante interne of externe omstandigheden, en eventuele keteneffecten op andere systemen of diensten. Deze context schetst een volledig beeld van de situatie, waardoor de impact en mogelijke vervolgmaatregelen beter kunnen worden beoordeeld.

Incident beschrijving

Leg de details van het beveiligingsincident uit, inclusief hoe het werd ontdekt, welke acties zijn ondernomen om het te beheersen en op te lossen, en de tijdlijn van de gebeurtenissen.

Beschrijf daarbij:

- Specifieke systemen of gegevens die door het incident zijn getroffen;
- Maatregelen voor beheersing en herstel, inclusief eventuele technische of procedurele aanpassingen die zijn doorgevoerd;
- De impact op de organisatie en haar stakeholders, zoals financiële schade, reputatieverlies of operationele verstoringen;
- De rol van menselijke fouten of organisatorische tekortkomingen die hebben bijgedragen aan het ontstaan of het verloop van het incident.

Een gedetailleerde en gestructureerde beschrijving van deze punten helpt bij het analyseren van de oorzaak, het beoordelen van de impact en het vaststellen van verbetermaatregelen om toekomstige incidenten te voorkomen.

Tijdslijn

Datum - tijd	Bevinding	Actie

Root cause analysis

Identificeer de onderliggende oorzaken van het incident en beschrijf de factoren die eraan hebben bijgedragen.

Dit kan onder meer omvatten:

- Technische kwetsbaarheden: Bijvoorbeeld verouderde software, onvoldoende patchmanagement, verkeerde configuraties of ontbrekende beveiligingsmaatregelen;
- Menselijke fouten: Zoals onjuiste handelingen, nalatigheid, gebrekkige training of onduidelijke procedures;
- Organisatorische tekortkomingen: Bijvoorbeeld een gebrek aan beleid of richtlijnen, onvoldoende toezicht, zwakke interne controles, of onvoldoende middelen voor beveiliging.

Door deze oorzaken en bijdragende factoren duidelijk in kaart te brengen, kan de organisatie gerichte verbetermaatregelen nemen om vergelijkbare incidenten in de toekomst te voorkomen.

Lessons learned

Beschrijf de belangrijkste lessen die uit het incident zijn getrokken en hoe deze kunnen worden gebruikt om de beveiligingspositie van de organisatie te versterken. Kijk hierbij onder andere naar:

- Wat hebben we goed gedaan?
- Wat kunnen we beter doen?

Het doorvoeren van geleerde lessen kan onder meer inhouden:

- Aanpassingen in beleid en procedures: Bijvoorbeeld het herzien van incidentresponsplannen, toegangsbeheer, patchmanagement of change-managementprocedures;
- Technische verbeteringen: Zoals het versterken van netwerkbeveiliging, het implementeren van geavanceerde monitoring- en detectietools, het verscherpen van configuratiestandaarden, of het automatiseren van updates;
- Training en bewustwordingsprogramma's: Gericht op medewerkers, zodat zij phishing, social engineering en andere dreigingen sneller herkennen en correct handelen.

Beoordeel daarbij ook:

- De effectiviteit van de bestaande beveiligingsmaatregelen, beleid en procedures
  - Welke onderdelen goed hebben gewerkt tijdens het incident;
  - Welke zwakke punten aan het licht zijn gekomen en welke verbeteringen noodzakelijk zijn.

Door deze lessen concreet vast te leggen en te vertalen naar actiepunten kan de organisatie toekomstige risico's verkleinen, incidentrespons versnellen en de algehele cyberweerbaarheid vergroten.

Aanbevelingen

Geef concrete aanbevelingen om vergelijkbare incidenten in de toekomst te voorkomen. Deze aanbevelingen kunnen onder meer omvatten:

Technische maatregelen en upgrades

- Implementeren van nieuwe technologieën: Zoals geavanceerde intrusion detection- en prevention-systemen (IDS/IPS), Security Information and Event Management (SIEM), of Endpoint Detection & Response (EDR);
- Versterken van beveiligingscontroles: Striktere patch- en updateprocedures, segmentatie van netwerken, multi-factor-authenticatie (MFA) en versleuteling van gevoelige data;
- Automatiseren van monitoring en incidentrespons: Bijvoorbeeld door real-time loganalyse en geautomatiseerde alerts in te richten.

Beleid, processen en governance

- Herzien en aanscherpen van beveiligingsbeleid en procedures: Duidelijke richtlijnen voor toegangsbeheer, change management en kwetsbaarhedenbeheer;
- Regelmatige interne audits en penetratietesten: Om zwakke plekken vroegtijdig te ontdekken en aan te pakken;
- Verbeteren van het incidentresponsplan: Inclusief duidelijke escalatieprocedures en communicatielijnen.

Training en bewustwording

- Gerichte beveiligingstrainingen voor IT-personeel en eindgebruikers: Onderwerpen: phishing, social engineering, veilig wachtwoordgebruik, en het herkennen van verdachte activiteiten;
- Simulaties en oefeningen: Bijvoorbeeld tabletop-exercises of red-team/blue-team-oefeningen om de paraatheid te testen;
- Continu bewustwordingsprogramma: Regelmatige updates, workshops en interne campagnes om het veiligheidsbewustzijn hoog te houden.

Verbeterkansen voor de beveiligingspositie

- Uitbreiding van technische beveiligingslagen (defense in depth);
- Beter risicobeheer en prioritering op basis van actuele dreigingsanalyses;
- Integratie van security by design bij nieuwe projecten en applicaties.

Door deze maatregelen te combineren – technisch, organisatorisch en mensgericht – kan de organisatie haar cyberweerbaarheid vergroten, het risico op herhaling van incidenten drastisch verminderen, en beter voldoen aan normen zoals ISO 27001 en CBW (NIS2).

Conclusie

Samenvatting van de belangrijkste punten van het rapport:

- Het incident is volledig geanalyseerd, inclusief context, tijdlijn en getroffen systemen of gegevens;
- De onderliggende oorzaken zijn vastgesteld, zoals mogelijke technische kwetsbaarheden, menselijke fouten of organisatorische tekortkomingen;
- De impact op de organisatie en haar stakeholders is in kaart gebracht, waaronder mogelijke financiële schade, reputatieverlies en operationele verstoringen;
- Er zijn lessons learned geformuleerd, met concrete verbeteringen voor beleid, processen, technische beveiligingsmaatregelen en training;

- Er zijn aanbevelingen gedaan om toekomstige incidenten te voorkomen, zoals technische upgrades, versterkte beveiligingscontroles, verbeterde governance en continue bewustwordingsprogramma's.

Belang van leren van beveiligingsincidenten
Het is cruciaal dat een organisatie systematisch leert van beveiligingsincidenten. Door incidenten te analyseren en hieruit duidelijke actiepunten te formuleren:

- Wordt de beveiligingspositie versterkt en het risico op herhaling aanzienlijk verminderd;
- Kan de incidentrespons worden versneld en verbeterd, waardoor de impact bij een toekomstig incident beperkt blijft;
- Voldoet de organisatie beter aan wet- en regelgeving zoals ISO 27001 en CBW (NIS2).

Door deze continue verbetercyclus – detecteren, analyseren, leren en verbeteren – kan de organisatie haar cyberweerbaarheid duurzaam verhogen en de belangen van klanten, partners en andere stakeholders optimaal beschermen.

Actielijst

Nummer	Omschrijving	Datum	Eigenaar

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)

Maart 2026