plan voor respons bij cyberincidenten

Sjabloon

# Dit document gebruiken

* Dit document bevat richtlijnen en voorbeelden die organisaties kunnen volgen om de ontwikkeling van hun eigen Cyber Incident Response Plan (CIRP) te ondersteunen. Het sjabloon is niet uitputtend. Het CIRP van elke organisatie moet worden aangepast aan de unieke werkomgeving, prioriteiten, middelen en verplichtingen. Sommige velden bevatten **voorbeeldtekst in groen**. Deze tekst is alleen bedoeld als voorbeeld en mag niet worden gebruikt als basis voor uw CIRP.
* Er is ook een extra CIRP-toolbox beschikbaar met checklists en sjablonen die kunnen worden gebruikt tijdens de ontwikkeling van je CIRP.

Inhoud

[Dit document gebruiken 2](#_Toc159584563)

[Autoriteit en herziening 3](#_Toc159584564)

[Documentcontrole en beoordeling 3](#_Toc159584565)

[Versiebeheer 3](#_Toc159584566)

[Doel en doelstellingen 4](#_Toc159584567)

[Standaarden en kaders 4](#_Toc159584568)

[Definities en acroniemen 4](#_Toc159584569)

[Incident response process flow 5](#_Toc159584570)

[Veelvoorkomende beveiligingsincidenten en reacties 6](#_Toc159584571)

[Terminologie en definities 6](#_Toc159584572)

[Veelvoorkomende bedreigingsvectoren 7](#_Toc159584573)

[Veelvoorkomende cyberincidenten 7](#_Toc159584574)

[Rollen en verantwoordelijkheden 8](#_Toc159584575)

[Contactpunten voor het melden van cyberincidenten 8](#_Toc159584576)

[Cyberincidentbestrijdingsteam (CIRT) 9](#_Toc159584577)

[Management Team (MT) 9](#_Toc159584578)

[Rollen en relaties 10](#_Toc159584579)

[Communicatie 10](#_Toc159584580)

[Interne communicatie 11](#_Toc159584581)

[Externe communicatie 11](#_Toc159584582)

[Ondersteunende procedures en draaiboeken 11](#_Toc159584583)

[Ondersteunende standaard operationele procedures (SOP's) 11](#_Toc159584584)

[Ondersteunende Playbooks 12](#_Toc159584585)

[Stakeholder Melding en rapportage van incidenten 12](#_Toc159584586)

[Incidentbestrijdingsproces 13](#_Toc159584587)

[Detectie, onderzoek, analyse en activering 13](#_Toc159584588)

[Incidentclassificatie 13](#_Toc159584589)

[vragen over incidentenonderzoek 14](#_Toc159584590)

[Escalatie en de-escalatie 14](#_Toc159584591)

[Insluiting, verzamelen van bewijsmateriaal en sanering 15](#_Toc159584592)

[Insluiting 15](#_Toc159584593)

[Documentatie 15](#_Toc159584594)

[Verzamelen en bewaren van bewijs 16](#_Toc159584595)

[Saneringsactieplan 16](#_Toc159584596)

[Herstel 17](#_Toc159584597)

[Geleerde lessen. 17](#_Toc159584598)

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
|  |  |  |  |

# Doel en doelstellingen

Beschrijf hier het doel van uw Cyber Incident Response Plan (CIRP).

*Bijvoorbeeld:*

*Het doel van dit CIRP is om een snelle en effectieve reactie op cyberincidenten te ondersteunen, afgestemd op de beveiligings- en bedrijfsdoelstellingen van de organisatie*.

*Doelstellingen van het CIRP*

* *Een leidraad bieden voor de stappen die nodig zijn om te reageren op cyberincidenten.*
* *De rollen, verantwoordelijkheden, verantwoordelijkheden en bevoegdheden van personeel en teams schetsen die nodig zijn om reacties op cyberincidenten te beheren.*
* *De vereisten voor naleving van wet- en regelgeving voor cyberincidenten schetsen.*
* *Interne en externe communicatieprocessen schetsen bij het reageren op cyberincidenten.*
* *Begeleiding bieden bij activiteiten na een incident ter ondersteuning van voortdurende verbetering.*

# Standaarden en kaders

De volgende documenten waarnaar wordt verwezen, zijn gebruikt als inspiratie om tot deze sjabloon te komen. De referenties zijn niet gedateerd. Hier geldt altijd de laatste uitgave van het document waarnaar wordt verwezen (inclusief eventuele wijzigingen).

* [CyberFundamentals Framework](https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework) [(](file:///C:\Users\Decock_Johan\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\WN18ZJI1\www.cyfun.be)www.cyfun.be)
* [NIST SP 800-61](https://csrc.nist.gov/pubs/sp/800/61/r2/final); Handleiding voor het afhandelen van beveiligingsincidenten bij computers
* ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 Incidentbeheer informatiebeveiliging.
* ISO/IEC 27001, Informatiebeveiliging, cyberveiligheid en privacybescherming - Beheersystemen voor informatiebeveiliging - Eisen
* ISO/IEC 27002, Informatiebeveiliging, cyberveiligheid en privacybescherming

Beheersystemen voor informatiebeveiliging - Beheersmaatregelen voor informatiebeveiliging.

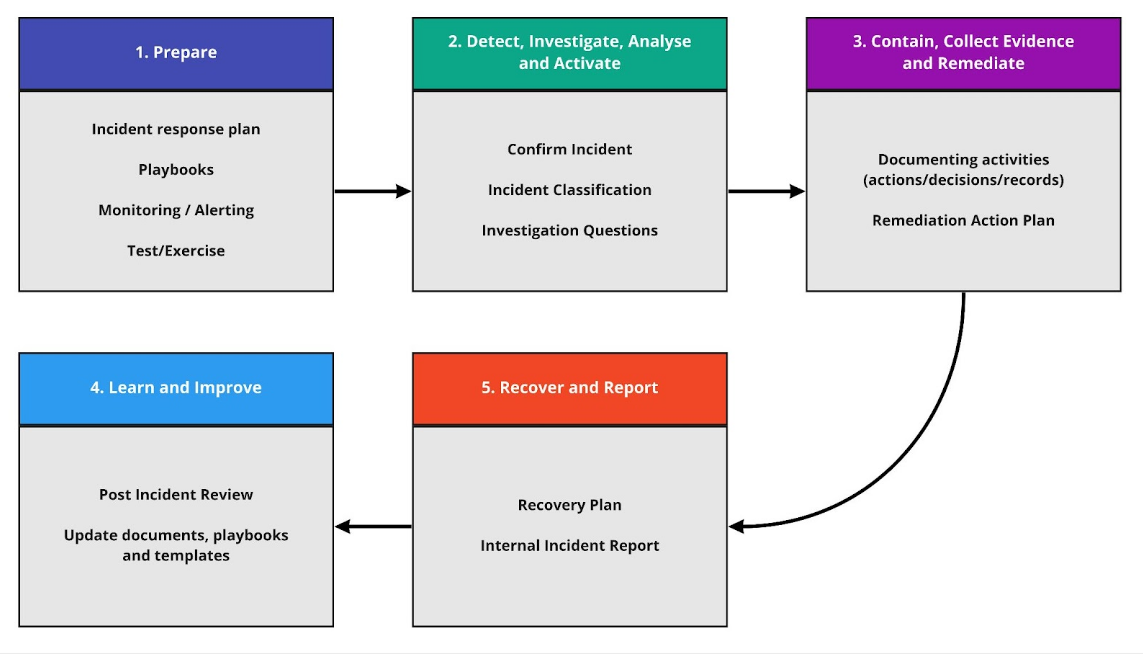
* Australisch Cyber Security Center, Cyber Incident Response-plan.

# Definities en acroniemen

In dit document zijn de termen en definities uit ISO/IEC 17000, ISO/IEC 27000 en volgende afkortingen van toepassing.

|  |  |
| --- | --- |
| **CEO** | Algemeen directeur |
| **CFO** | Financieel directeur |
| **CIO** | chief information officer |
| **CIRP** | Responsplan voor cyberincidenten |
| **CIRT** | Cyberincidentbestrijdingsteam |
| **CISO** | chief information security officer |
| **COO** | chief operating officer |
| **DDoS** | Distributed Denial-of-service |
| **DoS** | Denial-of-service |
| **DPO** | Functionaris voor gegevensbescherming |
| **GBA** | Gegevensbeschermingsautoriteit |
| **ICS** | Industrieel besturingssysteem |
| **MT** | Managementteam |
| **RPO** | Herstelpunt Doelstelling |
| **RTO** | Doelstelling hersteltijd |
| **SN** | Serienummer |
| **SPOC** | Eén aanspreekpunt |

# Incident response process flow



# Veelvoorkomende beveiligingsincidenten en reacties

## Terminologie en definities

Het gebruik van consistente en vooraf gedefinieerde terminologie om incidenten en hun gevolgen te beschrijven kan nuttig zijn tijdens een respons. Neem in uw Cyber Incident Response Plan (CIRP) veelgebruikte termen op die in uw organisatie worden gebruikt. Cyberbedreigingen, gebeurtenissen, waarschuwingen en incidenten worden als volgt gedefinieerd:

**Cyberdreiging**

Een cyberdreiging is elke omstandigheid of gebeurtenis die systemen of informatie kan beschadigen. Organisaties kunnen een lijst met zorgwekkende cyberbedreigingen opnemen. de volgende lijst toont de bedreigingsomgeving en de belangrijkste trends op het gebied van cyberbeveiliging:

* Phishing-e-mails en oplichting
* Ransomware
* Misbruik van zwakke plekken in de beveiliging
* Compromis over softwareleveringsketen
* Compromittering zakelijke e-mail
* Cybercriminaliteit

**Cyberveiligheidsevenement**

Een cyberbeveiligingsgebeurtenis is een gebeurtenis in een systeem, dienst of netwerktoestand die duidt op een mogelijke inbreuk op het beveiligingsbeleid, het falen van beveiligingen of een voorheen onbekende situatie die relevant kan zijn voor de beveiliging. Een cyberbeveiligingsincident kan een cyberincident worden, maar is dat nog niet.

Voorbeelden van cyberbeveiligingsgebeurtenissen zijn onder andere (maar niet beperkt tot):

* Een gebruiker heeft de antivirus op zijn computer uitgeschakeld
* Een gebruiker heeft systeembestanden verwijderd of gewijzigd
* Een gebruiker heeft een server opnieuw opgestart
* Onbevoegde toegang tot een server of systeem.

**Cyberbeveiligingswaarschuwing**

Een cyberbeveiligingswaarschuwing is een melding die wordt gegenereerd als reactie op een afwijking van normaal gedrag. Cyberbeveiligingswaarschuwingen worden gebruikt om cyberbeveiligingsgebeurtenissen onder de aandacht te brengen.

**Cyberincident**

Een cyberincident is een ongewenste of onverwachte cyberbeveiligingsgebeurtenis, of een reeks van dergelijke gebeurtenissen, die een aanzienlijke kans hebben om de bedrijfsactiviteiten in gevaar te brengen. Een cyberincident vereist corrigerende maatregelen.

Voorbeelden van cyberbeveiligingsincidenten zijn onder andere (maar niet beperkt tot):

* Denial-of-service-aanvallen (DoS)
* Onbevoegde toegang of pogingen tot toegang tot een systeem
* Compromittering van gevoelige informatie
* Uitbraak van virussen of malware (inclusief ransomware).

### Veelvoorkomende bedreigingsvectoren

De volgende tabel bevat veelvoorkomende bedreigingsvectoren uit de NIST Computer Security Incident Handling Guide.

|  |  |
| --- | --- |
| **Type** | **Beschrijving** |
| **Externe/verwijderbare media** | Een aanval uitgevoerd vanaf verwijderbare media of een randapparaat (bijv. kwaadaardige code die zich op een systeem verspreidt vanaf een geïnfecteerd USB-flashstation). |
| **Uitval** | Een aanval waarbij brute krachtmethoden worden gebruikt om systemen, netwerken of diensten in gevaar te brengen, aan te tasten of te vernietigen (bijvoorbeeld een DDoS die bedoeld is om de toegang tot een dienst of toepassing te belemmeren of te weigeren of een brute krachtaanval tegen een verificatiemechanisme, zoals wachtwoorden). |
| **Web** | Een aanval die wordt uitgevoerd vanaf een website of webgebaseerde toepassing (bijvoorbeeld een cross-site scripting aanval die wordt gebruikt om referenties te stelen of een omleiding naar een site die misbruik maakt van een kwetsbaarheid in de browser en malware installeert). |
| **E-mail** | Een aanval die wordt uitgevoerd via een e-mailbericht of bijlage (bijvoorbeeld exploitcode vermomd als een bijgevoegd document of een koppeling naar een schadelijke website in de hoofdtekst van een e-mail). |
| **Interdictie in de toeleveringsketen** | Een antagonistische aanval op hardware of software waarbij gebruik wordt gemaakt van fysieke implantaten, Trojaanse paarden of backdoors, door het onderscheppen en wijzigen van goederen die onderweg zijn van de verkoper of verkoper. |
| **Imitatie** | Een aanval waarbij iets goedaardigs wordt vervangen door iets kwaadaardigs (bijvoorbeeld spoofing, man in the middle-aanvallen, malafide draadloze toegangspunten en SQL-injectieaanvallen hebben allemaal te maken met impersonatie). |
| **Onjuist gebruik** | Elk incident dat het gevolg is van schending van het beleid voor aanvaardbaar gebruik van een organisatie door een geautoriseerde gebruiker, met uitzondering van de bovenstaande categorieën (bijv. een gebruiker installeert software voor het delen van bestanden, waardoor gevoelige gegevens verloren gaan). |
| **Verlies of diefstal van apparatuur** | Verlies of diefstal van een computerapparaat of -medium dat door een organisatie wordt gebruikt (bijvoorbeeld een laptop, smartphone of verificatietoken). |

### Veelvoorkomende cyberincidenten

De volgende tabel bevat een lijst met veelvoorkomende typen cyberincidenten en de bijbehorende eerste responsactiviteiten.  
 Beschrijf kort de eerste reactie op het incident. Bijvoorbeeld: stel relevante personen op de hoogte, isoleer getroffen apparaten, volg relevante playbooks en procedures.

|  |  |
| --- | --- |
| **Type/Omschrijving** | **Reactie** |
| **Denial of Service (DoS) en Distributed Denial of Service (DDoS):** een dienst overspoelen met verkeer, soms met gevolgen voor de beschikbaarheid. | *Zoals beschreven in afspeelboek X en procedures....., onderneem eerst lokale acties om het probleem op te lossen.*  *Als dit niet effectief is, volgens XYZ, vraag dan toestemming om te escaleren naar de tweede lijn, enz.* |
| **Phishing:** misleidende berichten om gevoelige informatie van gebruikers te ontlokken (zoals banklogins of zakelijke aanmeldgegevens) of om kwaadaardige code uit te voeren om toegang op afstand mogelijk te maken. | *Indien geïdentificeerd door personeel door succesvolle schadelijke inhoud*  *training, waarschuw en geef een kopie aan de beveiligingsbeambte. Schets volgende*  *acties en andere externe en interne notificatieacties, enz*. |
| **Ransomware:** een hulpprogramma dat wordt gebruikt om bestanden van slachtoffers te vergrendelen of te versleutelen totdat er losgeld wordt betaald. |  |
| **Malware:** een Trojaans paard, virus, worm of andere kwaadaardige software die een computersysteem of netwerk kan beschadigen. |  |
| **Inbreuk op gegevens:** onbevoegde toegang tot en openbaarmaking van informatie. |  |
| **Industrial Control System compromise:** ongeautoriseerde toegang tot ICS. |  |

# Rollen en verantwoordelijkheden

Dit onderdeel bevat details over de rollen en verantwoordelijkheden van de belangrijkste personen en teams die verantwoordelijk zijn voor incidentrespons en besluitvorming, waaronder het Cyber Incident Response Team (CIRT) op operationeel niveau en het Management Team (MT) op strategisch niveau.

Al het personeel dat hier wordt genoemd, moet bekend zijn met hun verantwoordelijkheden in dit plan en hun reactie oefenen.

### Contactpunten voor het melden van cyberincidenten

Primaire en secundaire (back-up) interne contactpunten om cyberincidenten aan te melden gedurende een 24/7 periode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Naam** | **Openingstijden** | **Contactgegevens** | **Titel** | **Verantwoordelijkheden** |
| *John Doe* | *09u00-18u00* | *Mobiel telefoonnummer,* | *Primair contact in geval van een incident* | *SPOC* |

### Cyberincidentbestrijdingsteam (CIRT)

Neem details op van het CIRT dat verantwoordelijk is voor het beheer van reacties op cyberincidenten. De samenstelling van uw CIRT zal variëren afhankelijk van de grootte van uw organisatie en de beschikbare vaardigheden en middelen. Vermeld details van externe leveranciers die uw ICT-systemen/toepassingen leveren of beheren. Vermeld, indien van toepassing, details over uw externe incident response providers en de diensten die zij leveren.

CIRT-leden die verantwoordelijk zijn voor het beheer van reacties op cyberincidenten:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Naam** | **Organisatie Rol** | **Contactgegevens** | **CIRT-rol Titel** | Verantwoordelijkheden CIRT |
|  |  |  | *Cyberincidentmanager* | *Planning van reacties*  *CIRT-operaties* |
|  |  |  | *netwerkingenieurs,* |  |
|  |  |  | *systeembeheerders,* |  |
|  |  |  |  |  |
|  |  |  |  |  |

Voor meer significante cyberbeveiligingsincidenten kan het CIRT worden uitgebreid:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Naam** | **Organisatie Rol** | **Contactgegevens** | **CIRT-rol Titel** | **Verantwoordelijkheden CIRT** |
|  |  |  | *Communicatiemanager* | *Informatie en waarschuwingen*  *Interne communicatie* |
|  |  |  | *Juridisch adviseur* | *Juridisch advies*  *(incl. naleving van regelgeving)* |
|  |  |  |  |  |

### Management Team (MT)

Significante cyberincidenten kunnen de vorming van het MT vereisen om strategisch toezicht, richting en ondersteuning te bieden aan het CIRT, met de nadruk op:

* Strategische kwesties identificeren en beheren
* Betrokkenheid bij en communicatie met belanghebbenden (inclusief contact met bestuur en ministeries, indien van toepassing)
* Vraag naar middelen en capaciteiten (inclusief dringende logistieke of financiële vereisten en personeelsoverwegingen tijdens de responsinspanning).

MT-leden die verantwoordelijk zijn voor het beheer van reacties op cyberincidenten:

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Contactgegevens** | **Titel** | **MT Rol** |
|  |  | *CEO* | *Stoel* |
|  |  | *CIO* | *Plaatsvervangend voorzitter* |
|  |  | *CISO* | *Beveiligingswaarschuwing en bewaking van CIA.* |
|  |  | *COO* | *Operationele functies van het bedrijf* |
|  |  | *CFO* | *Noodaankopen en toezicht op uitgaven* |
|  |  | *Juridische raad* | *Naleving van regelgeving, cyberverzekering* |
|  |  | *Communicatiemanager* | *Public relations en betrokkenheid van belanghebbenden* |
|  |  |  |  |

### Rollen en relaties

Het volgende schema geeft de relatie weer tussen het belangrijkste personeel en de teams die betrokken zijn bij de respons.



# Communicatie

Tijdens het reageren op incidenten is er voortdurend behoefte aan informatie van veel verschillende belanghebbenden. Elk van hen zal een ander soort informatie nodig hebben. Maak uw eigen lijst van potentiële belanghebbenden en zorg ervoor dat de juiste contactinformatie beschikbaar is! Merk op dat de organisatie deze contactinformatie beschikbaar moet hebben, maar niet altijd met alle partijen hoeft te communiceren.

Organisaties moeten er rekening mee houden dat wanneer een partij eenmaal op de hoogte is gesteld, zij zal vragen om periodieke updates met betrekking tot het incident in kwestie. Er is meestal geen sprake van eenmalige communicatie en het communicatieschema moet rekening houden met deze periodieke updates.

De eerste stap in uw incident-specifiek communicatieplan is bepalen met wie u gaat communiceren. Om dit te kunnen doen, moet u bepalen welke potentiële belanghebbenden (nadelige) gevolgen kunnen ondervinden van het cyberbeveiligingsincident waarmee u wordt geconfronteerd en of u wettelijk verplicht bent om bepaalde entiteiten op de hoogte te stellen.

* Interne belanghebbenden: topmanagement, beïnvloede managers, werknemers
* Externe belanghebbenden: media, klanten, leveranciers, andere partners, enz.
* Officiële belanghebbenden: GBA, toezichthouder voor de sector, politie,....

Wanneer u bepaalt wat u gaat communiceren en met wie, is een goede vuistregel om alleen te communiceren op een 'need-to-know' basis. Er zullen belanghebbenden zijn met wie u wilt communiceren om het cyberbeveiligingsincident in te dammen, en er zullen belanghebbenden zijn met wie u moet communiceren, omdat ze u om informatie vragen (bijv. de media) of omdat u wettelijk verplicht bent hen op de hoogte te stellen.

### Interne communicatie

*Begeleiding:*

Naast regelmatige situatierapporten kan het nodig zijn om medewerkers van uw organisatie te informeren over een cyberincident. Dit is belangrijk als de IT-netwerken, besturingssystemen of applicaties van de organisatie niet meer werken zoals verwacht, of als de situatie media- of publieke belangstelling kan genereren.

De belangrijkste boodschappen voor werknemers zijn onder andere

* Wat is er gebeurd en waarom?
* Wat zal er in de nabije toekomst gebeuren?
* Wat wordt er van werknemers verwacht?
* Met wie kunnen werknemers contact opnemen als ze vragen hebben?

### Externe communicatie

*Begeleiding:*

Afhankelijk van de impact en de ernst van een cyberincident kan het nodig zijn om te communiceren met externe belanghebbenden (waaronder ministers, media en het publiek). Dit is vooral belangrijk als het incident invloed heeft op IT-netwerken, controlesystemen of toepassingen waarop derden vertrouwen, zoals websites of diensten voor het publiek.

Belangrijke boodschappen om te overwegen bij de communicatie met externe belanghebbenden zijn onder andere:

* Wat is er gebeurd en waarom?
* Welke systemen/services worden beïnvloed?
* Welke stappen worden er ondernomen om de situatie op te lossen?
* Is het mogelijk om te zeggen wanneer de situatie zal worden opgelost?
* Wat wordt er verwacht van externe belanghebbenden?
* Met wie kunnen externe belanghebbenden contact opnemen als ze vragen/zorgen hebben?

**Alle communicatie moet worden beoordeeld en goedgekeurd door *de communicatieverantwoordelijke en de Incident Manager* voordat deze wordt vrijgegeven.**

# Ondersteunende procedures en draaiboeken

### Ondersteunende standaard operationele procedures (SOP's)

De Standard Operating Procedures (SOP's) die beschikbaar zijn om de respons op incidenten te ondersteunen:

* *Detectie, triage en analyse van gebeurtenissen*
* *Bedrijfscontinuïteitsplan*
* *Disaster Recovery Plan.*

### Ondersteunende Playbooks

De beschikbare playbooks bieden stapsgewijze richtlijnen voor reacties op veelvoorkomende incidenten:

* *Draaiboek voor respons bij cyberbeveiligingsincidenten -* ***Phishing***
* *Draaiboek voor respons bij cyberbeveiligingsincidenten* ***- gegevensinbraak/diefstal***
* *Draaiboek voor respons bij cyberbeveiligingsincidenten* ***- Malware***
* *Draaiboek voor respons bij cyberbeveiligingsincidenten* ***- Ransomware***
* *Cyber Security Incident Response Playbook* ***- Denial of Service.***

# Stakeholder Melding en rapportage van incidenten

Processen voor interne en externe melding en rapportage van incidenten omvatten:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type incident/**  **drempel** | **Organisatie  die een melding  of rapport wil  ontvangen** | **Contactgegevens  van de aanmeldende organisatie.** | **Belangrijkste meldings- en rapportagevereisten en koppeling met organisatie-informatie** | **Verantwoordelijk personeel** |
| Ransomware | Centrum voor Cyberveiligheid België. CERT.BE | info@ccb.belgium.be | https://www.cert.be/en/report-incident-0 | Cyberincidentmanager |
| Inbreuk op persoonlijke gegevens | Gegevensbeschermings-autoriteit | +32 (0)2 274 48 00  +32 (0)2 274 48 35  contact@apd-gba.be | https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens | Juridisch adviseur of DPO |

* **maak een lijst van de wettelijke en reglementaire vereisten voor je bedrijf.**
* **Als er een cyberverzekeringspolis is, controleer dan de vereisten in de verzekering om er zeker van te zijn dat je eraan voldoet.**

# Incidentbestrijdingsproces

# Detectie, onderzoek, analyse en activering

Raadpleeg uw eigen standaard operationele procedures voor het detecteren, onderzoeken en analyseren van incidenten. Hierin kan worden opgenomen hoe u zich bewust wordt van een gebeurtenis of incident en wat u onmiddellijk doet als reactie.

Incidenten kunnen op verschillende manieren worden gedetecteerd, waaronder, maar niet beperkt tot:

* Zelfgedetecteerde incidenten (bijv. Intrusion Detection and Prevention-systemen)
* Kennisgevingen ontvangen van serviceproviders of verkopers
* Meldingen ontvangen van vertrouwde derden zoals het Centrum voor Cyberveiligheid België, MITRE ATT&CK, ENISA....

### Incidentclassificatie

Dit kan helpen bij het prioriteren van middelen. Classificatiefactoren kunnen zijn:

* Gevolgen van het incident (vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen)
* Betrokken belanghebbenden (intern en extern)
* Type incident
* Impact op het bedrijf en de gemeenschap.

|  |  |
| --- | --- |
| **Classificatie van incidenten** | **Beschrijvingen** |
| **Kritisch** | *Een kritiek incident met een zeer grote impact. Het gaat vaak om een volledige systeemuitval, verlies van klantgegevens, grote beveiligingslekken of kritieke infrastructuurstoringen.* |
| **Hoog** | *Een groot incident met een aanzienlijke impact. Het kan gedeeltelijke systeemstoringen omvatten of kritieke functionaliteiten aantasten.* |
| **Medium** | *Een matig incident met een matige impact dat invloed kan hebben op niet-kritieke functionaliteiten of ongemakken kan veroorzaken voor gebruikers.* |
| **Laag** | *Een klein incident met een lage impact dat kan bestaan uit niet-kritieke functiestoringen of klachten van gebruikers met een lage prioriteit.* |

### vragen over incidentenonderzoek

Een lijst met onderzoeksvragen kan u helpen bij uw inspanningen om te reageren op een incident en om inzicht te krijgen in de omvang en impact van het incident. Niet alle vragen kunnen worden beantwoord met de beschikbare gegevens en vragen kunnen veranderen naarmate het onderzoek vordert.

* *Wie heeft het incident ontdekt of gemeld?*
* *Wanneer werd het incident ontdekt of gemeld?*
* *Waar is het incident ontdekt of gelokaliseerd?*
* *Welke impact heeft het incident op de bedrijfsvoering?*
* *Wat is de omvang van het incident met het netwerk en de applicaties?*

### Escalatie en de-escalatie

Cyberincidenten kunnen worden geëscaleerd of gedeëscaleerd. De rollen die kunnen escaleren of de-escaleren moeten in een tabel worden opgenomen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Classificatie van incidenten** | **Actie** | **Reden voor escalatie / de-escalatie** | **Beslisser** |
|  |
| **Kritisch** | De-escaleren naar hoog |  |  |  |
| **Hoog** | Escaleren naar kritiek |  |  |  |
| De-escaleren naar gemiddeld |  |  |  |
| **Medium** | Escaleren naar hoog |  |  |  |
| De-escaleren naar laag |  |  |  |
| **Laag** | Escaleren naar gemiddeld |  |  |  |

# Insluiting, verzamelen van bewijsmateriaal en sanering

### Insluiting

Inperking is belangrijk voordat een incident de middelen overweldigt of de schade vergroot. De meeste incidenten moeten worden ingedamd, dus dat is een belangrijke overweging in een vroeg stadium van de afhandeling van elk incident. Inperking biedt tijd voor het ontwikkelen van een op maat gemaakte herstelstrategie. Een essentieel onderdeel van indamming is besluitvorming (bijvoorbeeld een systeem afsluiten, loskoppelen van een netwerk, bepaalde functies uitschakelen). Dergelijke beslissingen zijn veel gemakkelijker te nemen als er vooraf bepaalde strategieën en procedures zijn voor het indammen van het incident. Organisaties moeten aanvaardbare risico's definiëren bij het omgaan met incidenten en dienovereenkomstig strategieën ontwikkelen.

Insluitingsstrategieën variëren afhankelijk van het type incident. Zo is de strategie voor het indammen van een malware-infectie via e-mail heel anders dan die voor een DDoS-aanval via een netwerk. Organisaties moeten aparte indammingsstrategieën opstellen voor elk belangrijk incidenttype, met duidelijk gedocumenteerde criteria om de besluitvorming te vergemakkelijken. Criteria voor het bepalen van de juiste strategie zijn onder andere:

* Mogelijke schade aan en diefstal van hulpbronnen
* Behoud van bewijsmateriaal
* Beschikbaarheid van diensten (bijv. netwerkconnectiviteit, diensten geleverd aan externe partijen)
* Tijd en middelen die nodig zijn om de strategie te implementeren
* Effectiviteit van de strategie (bijv. gedeeltelijke insluiting, volledige insluiting)
* Duur van de oplossing (bijv. noodoplossing die binnen vier uur moet worden verwijderd, tijdelijke oplossing die binnen twee weken moet worden verwijderd, permanente oplossing).

In bepaalde gevallen leiden sommige organisaties de aanvaller door naar een sandbox (een vorm van insluiting) zodat ze de activiteiten van de aanvaller kunnen monitoren, meestal om aanvullend bewijs te verzamelen. Het incident response team moet deze strategie bespreken met de juridische afdeling om te bepalen of het haalbaar is. Andere manieren om de activiteiten van een aanvaller te monitoren dan sandboxing zouden niet gebruikt moeten worden; als een organisatie weet dat een systeem gecompromitteerd is en de compromittering door laat gaan, kan het aansprakelijk gesteld worden als de aanvaller het gecompromitteerde systeem gebruikt om andere systemen aan te vallen. De strategie van uitgestelde indamming is gevaarlijk omdat een aanvaller ongeautoriseerde toegang kan escaleren of andere systemen kan compromitteren.

Een ander potentieel probleem met betrekking tot indamming is dat sommige aanvallen extra schade kunnen veroorzaken als ze ingedamd zijn. Een gecompromitteerde host kan bijvoorbeeld een kwaadaardig proces draaien dat periodiek een andere host pingt. Wanneer de incident handler het incident probeert te beperken door de gecompromitteerde host los te koppelen van het netwerk, zullen de volgende pings mislukken. Als gevolg van deze mislukking kan het kwaadaardige proces alle gegevens op de harde schijf van de host overschrijven of versleutelen. Behandelaars moeten er niet van uitgaan dat, alleen omdat een host is losgekoppeld van het netwerk, verdere schade aan de host is voorkomen.

### Documentatie

Het documenteren van alle gerelateerde informatie over het incident is essentieel. De volgende lijst is een indicatie van relevante informatie die moet worden gedocumenteerd. Als er rapporten worden gemaakt voor het management of andere belanghebbenden, moet deze informatie in het rapport staan.

* Datum en tijd incident
* Huidige status van het incident
* Contactgegevens van relevante personen (incidentmanager, CISO, CEO, ....)
* Reikwijdte en impact
* Ernst
* Type incident en classificatie
* Externe hulp nodig? JA / NEE. Vermeld contactgegevens.
* Acties die zijn ondernomen om het incident in te dammen en op te lossen.
* Informatie over de volgende update van het incident (datum, tijd, wie wordt geïnformeerd)

### Verzamelen en bewaren van bewijs

Houd bij het verzamelen van bewijsmateriaal een gedetailleerd logboek bij waarin duidelijk wordt gedocumenteerd hoe al het bewijsmateriaal is verzameld. Dit moet bevatten wie het bewijs heeft verzameld of behandeld, het tijdstip waarop het bewijs is verzameld en behandeld, en de details van elk verzameld item (inclusief de fysieke locatie, serienummer, modelnummer, hostnaam, logbestanden, IP-adres, besturingssysteem, ....).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum, tijd van verzamelen** | **Verzameld door** | **Bewijsmateriaal Details** | **Locatie van bewijsmateriaal** | **Toegang** |
| *01/01/2024* | *De heer Janssens* | *Harde schijf van laptop met SN, modelnr* | *Schijf met SN....*  *Opgeslagen in kluis in serverruimte* | *ICT-manager, CIRT-team* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Saneringsactieplan

Een actieplan opstellen om het incident op te lossen, na succesvolle insluiting en verzameling van bewijsmateriaal.

Bij het opstellen van het herstelactieplan kun je overwegen om de volgende vragen te beantwoorden. Deze vragen zijn beperkt, slechts een indicatie.

* Welke acties zijn nodig om het incident op te lossen?
* Welke middelen (intern & extern) zijn nodig om het incident op te lossen?
* Wie is de eigenaar van het incident dat wordt opgelost?
* Is er een prioriteit voor systemen of diensten die nodig zijn om het incident op te lossen?
* Op wie en wat heeft de resolutie invloed?
* Wat is het tijdschema voor het afsluiten van het incident?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum, tijd van het incident** | **Categorie**  **(Beheersen, herstellen,...)** | **Actie** | **Actie eigenaar** | **Status**  **(niet toegewezen, wordt aan gewerkt, gesloten)** |
| *01/01/2024* | *Bevat* | *Koppel de geïnfecteerde host los van het netwerk.* | *Systeembeheerder (inclusief naam)* | *In uitvoering* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Herstel

Maak herstelplannen voor verschillende scenario's. Het herstelplan moet in detail de aanpak beschrijven voor het herstellen van IT- en/of OT-netwerken, -systemen en -toepassingen zodra de insluiting en sanering is voltooid.

Houd bij het ontwikkelen van een herstelplan rekening met het volgende:

* de Recovery Time Objective (RTO) & Recovery Point Objective (RPO).
* Creëer een proces voor het bewaken van de systemen om te garanderen dat ze niet langer gecompromitteerd zijn en werken zoals verwacht.
* Wat kan er worden geïmplementeerd om soortgelijke incidenten te voorkomen?

# Geleerde lessen.

Een van de belangrijkste onderdelen van incident response wordt ook het vaakst overgeslagen: leren en verbeteren. Elk incidentresponsteam moet evolueren om nieuwe bedreigingen, verbeterde technologie en geleerde lessen te weerspiegelen. Het houden van een "lessons learned" bijeenkomst met alle betrokken partijen na een groot incident, en eventueel periodiek na kleinere incidenten als de middelen het toelaten, kan zeer nuttig zijn bij het verbeteren van beveiligingsmaatregelen en het incidentafhandelingsproces zelf. Meerdere incidenten kunnen worden besproken tijdens één "geleerde lessen"-bijeenkomst. Deze bijeenkomst biedt de mogelijkheid om een incident af te sluiten door te bespreken wat er is gebeurd, wat er is gedaan om in te grijpen en hoe goed de interventie heeft gewerkt. De bijeenkomst moet binnen enkele dagen na afloop van het incident worden gehouden.

Vragen die tijdens de bijeenkomst beantwoord moeten worden zijn onder andere:

* Wat is er precies gebeurd en op welke tijdstippen?
* Hoe goed hebben personeel en management het incident afgehandeld? Werden de gedocumenteerde procedures gevolgd? Waren ze adequaat?
* Welke informatie was eerder nodig?
* Zijn er stappen of acties ondernomen die het herstel mogelijk hebben belemmerd?
* Wat zouden het personeel en het management anders doen als een soortgelijk incident zich de volgende keer voordoet?
* Hoe had het delen van informatie met andere organisaties kunnen worden verbeterd?
* Welke corrigerende maatregelen kunnen soortgelijke incidenten in de toekomst voorkomen?
* Op welke voorlopers of indicatoren moet in de toekomst worden gelet om soortgelijke incidenten op te sporen?

Bijeenkomsten over geleerde lessen hebben nog andere voordelen. Verslagen van deze bijeenkomsten zijn goed materiaal voor het trainen van nieuwe teamleden door hen te laten zien hoe meer ervaren teamleden reageren op incidenten. Het bijwerken van het beleid en de procedures voor het reageren op incidenten is een ander belangrijk onderdeel van het leerproces. Een post-mortem analyse van de manier waarop een incident werd afgehandeld zal vaak een ontbrekende stap of een onnauwkeurigheid in een procedure aan het licht brengen, wat de aanzet geeft tot verandering. Vanwege de veranderende aard van informatietechnologie en veranderingen in het personeel, moet het incident response team alle gerelateerde documentatie en procedures voor het afhandelen van incidenten op gezette tijden herzien.

**Het regelmatig testen van het Cyber Incident Response Plan is belangrijk om ervoor te zorgen dat deze documenten actueel blijven en bekend zijn bij het relevante personeel. Testmethodes kunnen bijvoorbeeld discussie of functionele oefeningen zijn.**

**Cyber Incident Response Plan trainingsoefeningen van verschillende scenario's zijn van grote waarde om meer en meer informatie te krijgen uit de geleerde lessen. Tijdens deze testscenario's kan er veel informatie ontbreken of worden processen niet uitgevoerd zoals gedefinieerd. Dit zijn geweldige uitkomsten, zodat je de procedures en processen kunt aanpassen voor wanneer je het cyber incident response plan echt nodig hebt!**