Informatieclassificatie Vlaamse overheid

Incidentbeheer

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

Classificatie: Klasse 2

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen beheer van incidenten. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 4 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de deel al de nodige aanvullende informatie ter beschikking wordt gesteld, vervolgens bespreken we de link met andere maatregelen. Het document wordt afgerond met de prestatie indicatoren.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.0.1	8 mei 2019	Kristel VAN AKEN	Draft
v.0.2	21 mei 2019	Kristel VAN AKEN	Draft bijgewerkt na overleg op 20 mei
v.0.3	26 juni 2019	Kristel VAN AKEN	Feedback taakgroep
v.0.4	29 juli 2019	Kristel VAN AKEN	Feedback taakgroep event management
v.1.0	29 juli 2019	Kristel VAN AKEN	Versie gepubliceerd in pdf
v.1.1	20 maart 2020	Kristel VAN AKEN	Versie gepubliceerd in pdf
v.1.2	21 januari 2021	Beau JANSSEN	Toevoeging Integriteit als kwaliteitskenmerk
v.2.0	19 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
v.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van de volgende documenten:

Documentverwijzingen:

- *Vo Informatieclassificatie – Organisatie Informatieveiligheid* (PDF)
- *Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk* (PDF)
- Vo Informatieclassificatie – Minimale maatregelen (PDF):
  - *Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – beheer gebeurtenissen*
  - *Vo Informatieclassificatie - Minimale maatregelen – probleembeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – release en deployment beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

Inhoudsopgave

INLEIDING

Het proces incident beheer

Het doel van incident beheer is om verstoringen in de infrastructuur en dienstverlening te verhelpen en gebruikersvragen te beantwoorden, teneinde zo snel mogelijk het normale/ gewenste niveau van de dienstverlening te herstellen.

Deze dienstverlening wordt vaak in een overeenkomst – de SLA (*Service Level Agreement*) – in detail beschreven.

Beheren en opvolgen van incidenten is belangrijk omdat 100% beveiligen niet mogelijk is: incidenten zijn niet te voorkomen, het is een kwestie van wanneer niet of.

Het proces 'beheer van incidenten' gaat van de detectie en aanname van een melding tot het verhelpen en afsluiten van de storing in afstemming met de gebruiker.

Incident beheer op gebied van informatiebeveiliging omvat de monitoring en detectie van informatie veiligheidsincidenten en maakt deel uit van het globale proces 'beheer van incidenten'.

Incident beheer in het kader van informatieclassificatie

Informatieclassificatie wordt uitgedrukt in drie kwaliteitskenmerken, men spreekt dan over:

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

Merk op dat in een eerste fase van het project informatieclassificatie de focus ligt op vertrouwelijkheid en technische integriteit (functionele integriteit en beschikbaarheid zullen later ingevuld worden); beschikbaarheid wordt inherent meegenomen in de scope van incident beheer maar er worden geen maatregelen uitgewerkt (dit wordt opgenomen in het programma bedrijfscontinuïteit).

Incident beheer in het kader van informatieclassificatie is dus het beheer van informatie veiligheidsincidenten, namelijk voortkomend uit informatie verwerkende zakelijke processen en hun ondersteunende infrastructuur/processen. Het proces incidentbeheer is hiervoor omkaderend: immers, veiligheidsincidenten zijn ook incidenten.

Hoewel het proces om beide types incidenten op te lossen analoog verloopt zijn er toch verschillen:

- (Informatie)veiligheidsincidenten zijn vaak (maar niet altijd) kwaadwillend of het resultaat van non-conformiteit aan de beleidslijnen;
- De scope is anders;
- De vaardigheden nodig om de situatie te herstellen zijn vaak erg verschillend.

Volgende tabel schetst het verschil tussen ICT-incidenten en informatie veiligheidsincidenten:

	ICT incident	*Informatie veiligheidsincident*
Definitie	• Vermindering of onderbreking van een ICT-dienst; • Niet kwaadwillig.	Aantasting van vertrouwelijkheid, integriteit of beschikbaarheid van de informatievoorziening; • Vaak kwaadwillig; • Of non-conformiteit met beleidslijnen.
Doel	Herstel van de ICT-dienst	Herstel van de informatievoorziening
Scope	ICT-dienstverlening	Kan de volledige organisatie omvatten
Vaardigheden	ICT-technologie	ICT en bijkomende kennis zoals juridisch, forensics, enz.

1. MINIMALE MAATREGELEN

Het omgaan en beheren van incidenten omvat een aantal activiteiten die, afhankelijk van de klasse waartoe de getroffen informatie behoort, al dan niet verplicht uitgevoerd moeten worden. Deze activiteiten zijn (zie hoofdstuk: '*De bouwstenen van incident beheer*'):

- Melden van een incident;
- Toewijzen van een categorie aan het incident;
- Impact van het incident bepalen;
- Urgentie van het incident bepalen;
- Registratie en documentatie van het incident;
- Functionele escalatie;
- Hiërarchische escalatie;
- Communicatie van het incident;
- Inperken van de gevolgen van het incident;
- Uitvoeren van een *work around*;
- Uitwerken van een permanente oplossing via wijzigingsbeheer;
- Rapporteren van het incident;
- Uitvoeren van *lessons learned*.

De minimale beschikbaarheid van het proces 'incident beheer' zelf is eveneens afhankelijk van het type en klasse van de getroffen informatie. We onderscheiden beschikbaarheid tijdens kantooruren (10ux5dagen) en permanente beschikbaarheid (24ux7dagen).

Melden van een incident

Deze activiteit betreft gebruikers die een incident opmerken, het gaat dus niet om systeem meldingen (deze komen via het proces 'beheer van gebeurtenissen' in het incident registratiesysteem).

Voor het melden van incidenten moet een meldpunt voorzien worden. Dit kan een helpdesk/service desk zijn, maar even goed een teamleider of ICT-correspondent (een ICT-medewerker of een gebruiker aangeduid om informatie over incidenten te verzamelen.

Voor meer detail zie hoofdstuk: '*Helpdesk/service desk'*.

Toewijzen van een categorie

Dit is besproken in hoofdstuk '*Registratie en categorisatie van het incident*'.

Bepalen van de impact

Dit is besproken in hoofdstuk '*Prioriteit bepalen van een incident*'.

Bepalen van de urgentie

Dit is besproken in hoofdstuk '*Prioriteit bepalen van een incident*'.

Noteer dat impact en urgentie samen de prioriteit van het incident definiëren.

Registratie en documentatie van het incident

Met de registratie van een incident bedoelen we één of andere vorm van inschrijving. Daarnaast moet het incident ook gedocumenteerd worden. De eenvoudigste vorm is de registratie en documentatie in een logboek. Zo'n logboek kan bijgehouden worden door een afdeling of departement (decentraal) of centraal, al dan niet onder beheer van de incident manager. Voor de registratie, documentatie en opvolging van incidenten zijn diverse tools op de markt beschikbaar, maar deze zijn vaak duur en vereisen complexe installaties.

Voor meer detail zie hoofdstuk '*Registratie en categorisatie van het incident*' en hoofdstuk '*Documentatie van het incident*'.

Functionele escalatie

Vaak worden dezelfde incidenten meerdere malen gemeld en opgelost. Indien de oplossing of *work around* gekend is door het meldpunt, is het niet nodig om anderen in te schakelen. Indien er geen oplossing of *work around* gekend is door het meldpunt, moeten één of meerdere technische specialisten zich buigen over het incident. Het incident wordt hierbij waar nodig opgesplitst in deelincidenten die naar de betrokken afhandelaars worden gestuurd.

Voor meer detail zie hoofdstuk: '*Escalatie*'.

Hiërarchische escalatie

Sommige incidenten moeten doorgestuurd worden naar de security officer (CISO), ICT-coördinator of DPO (functionaris gegevensbescherming) indien aanwezig, dit laatste met name als er persoonsgegevens betrokken (kunnen) zijn bij het incident. Deze zal niet als primaire afhandelaar optreden (het technisch verhelpen gebeurt niet door de CISO of DPO), maar moet wel geïnformeerd worden.

Sommige incidenten vereisen een doorsturen naar het management, bijvoorbeeld wanneer de ernst van het incident zodanig hoog is of als er acties nodig zijn die de bevoegdheid van de betrokken medewerkers overstijgen.

Voor meer detail zie hoofdstuk: '*Escalatie*'.

Communicatie van het incident

Dit is besproken in hoofdstuk '*Communicatie van het incident*'.

Inperken van de gevolgen van het incident

Dit is besproken in hoofdstuk: '*Beperken van de schade*'.

Uitvoeren van *work around*

Wanneer het incident niet kan snel genoeg kan worden opgelost, is het soms toch mogelijk om een *work around* oplossing voor te stellen. Dit betekent dat de oorzaak van het incident niet is weggenomen, maar dat er een werkwijze kan worden voorgesteld om aan de gebruiker toe te laten dezelfde of een gedeeltelijke (aanvaardbare) functionaliteit te gebruiken tot een permanente oplossing gevonden en geïmplementeerd is.

Voor meer detail zie hoofdstuk: 'Behandelen van het incident'.

Uitwerken van een permanente oplossing via wijzigingsbeheer

Een incident kan vaak enkel opgelost worden (wegnemen van de oorzaak, inperken van de gevolgen) door het uitvoeren van een wijziging. Dit kan een eenvoudige systeemwijziging zijn (een verandering in de configuratie) of de uitvoering/implementatie van een complexe oplossing. Een wijziging kan enkel uitgevoerd worden onder het proces 'wijzigingsbeheer' (Voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer*')

Voor meer detail zie hoofdstuk: '*Behandelen van het incident*'.

Rapporteren van het incident

Dit is besproken in hoofdstuk '*Rapportering en evaluatie*'.

Uitvoeren van *lessons learned*

Een *lessons learned* oefening houdt een evaluatie van de afhandeling van het incident in. Dit is geen beoordeling van het proces 'incident beheer', maar een evaluatie van het incident zelf. Had dit voorkomen kunnen worden? Zijn er wijzigingen of verbeteroplossingen in de toekomst nodig?

Een *lessons learned* kan resulteren in een verbetertraject. Dit kan een verstrenging van procedures inhouden, een bewustmakingscampagne, technische implementaties, … Wanneer zo'n verbetertraject een wijziging inhoudt, dan dient dit opgenomen te worden door het proces wijzigingsbeheer indien het verbetertraject effectief ingepland dient te worden, of door het proces *release management* indien het verbetertraject opgenomen dient te worden maar nog niet effectief ingepland kan worden (bvb omdat bepaalde infrastructuur nog ontbreekt, of de impact op performantie nog te groot is of …).

Het is van belang dat de *lessons learned* oefening snel na het afsluiten van het incident plaats vindt, zodat alles nog vers in het geheugen is.

Dit is besproken in hoofdstuk '*Rapportering en evaluatie*'.

1.1. Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Melden van een incident aan een meldpunt; 〉 Toewijzen van een categorie aan het incident; 〉 Impact van het incident: geen of lage impact; 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen; 〉 Registratie en documentatie van het incident minimaal in een logboek; 〉 Functionele escalatie indien het meldpunt het incident niet kan oplossen; 〉 Escalatie naar management van incidenten met prioriteit P1; 〉 Communicatie van het incident naar de getroffen gebruikers; 〉 Inperken van de gevolgen van het incident; 〉 Uitvoeren van een *work around* indien beschikbaar; 〉 Uitwerken van een permanente oplossing en deze indienen als wijziging indien beschikbaar; 〉 Rapporteren van het incident; 〉 Uitvoeren van *lessons learned* voor incidenten met prioriteit P1 na afsluiten van het incident.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Impact van het incident: minimaal medium (want er is materiële schade mogelijk); 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen maar minimaal medium; 〉 Registratie van het incident in een centraal logboek onder beheer van een incident manager; 〉 Escalatie naar CISO/ICT-coordinator; 〉 Uitvoeren van *lessons learned* na afsluiten van het incident.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Impact van het incident: hoge impact (want hoge materiële schade mogelijk); 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen, minimaal medium; 〉 Functionele escalatie van elk incident; 〉 Uitvoeren van *lessons learned* na afsluiten van het incident en met verplicht verbetertraject via wijzigingsbeheer.

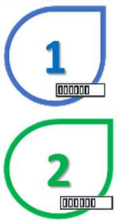
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Impact van het incident: hoge impact (want ernstige materiële schade mogelijk); 〉 Urgentie van het incident: altijd hoog; 〉 Escalatie naar management van elk incident.

Integriteit

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Melden van een incident aan een meldpunt; 〉 Toewijzen van een categorie aan het incident; 〉 Impact van het incident: geen of lage impact; 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen; 〉 Registratie en documentatie van het incident minimaal in een logboek; 〉 Functionele escalatie indien het meldpunt het incident niet kan oplossen; 〉 Escalatie naar management van incidenten met prioriteit P1; 〉 Communicatie van het incident naar de getroffen gebruikers; 〉 Inperken van de gevolgen van het incident; 〉 Uitvoeren van een *work around* indien beschikbaar; 〉 Uitwerken van een permanente oplossing en deze indienen als wijziging indien beschikbaar; 〉 Rapporteren van het incident; 〉 Uitvoeren van *lessons learned* voor incidenten met prioriteit P1 na afsluiten van het incident.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Impact van het incident: minimaal medium (want er is materiële schade mogelijk); 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen maar minimaal medium; 〉 Registratie van het incident in een centraal logboek onder beheer van een incident manager; 〉 Escalatie naar CISO/ICT coordinator; 〉 Uitvoeren van *lessons learned* na afsluiten van het incident.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Impact van het incident: hoge impact (want hoge materiële schade mogelijk); 〉 Urgentie van het incident bepalen: dit is afhankelijk van het type of aantal getroffen gebruikers of systemen, minimaal medium;

	〉 Functionele escalatie van elk incident; 〉 Uitvoeren van *lessons learned* na afsluiten van het incident en met verplicht verbetertraject via wijzigingsbeheer.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Impact van het incident: hoge impact (want ernstige materiële schade mogelijk); 〉 Urgentie van het incident: altijd hoog; 〉 Escalatie naar management van elk incident.

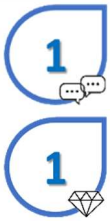
Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: Beschikbaarheid van het proces incidentbeheer is minimaal kantooruren (5d x 10u)
	Klasse 3, Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Beschikbaarheid van het proces incidentbeheer is minimaal kantooruren (24u x 7d)

1.2. Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor incidentbeheer moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk 'minimale algemene maatregelen').

Vertrouwelijkheid en integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1.
	Maatregelen voor Klasse 2: 〉 Escalatie naar CISO/ICT coördinator of DPO; 〉 Communicatie van het incident naar de getroffen burgers volgens de criteria van GDPR.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Escalatie naar DPO indien aanwezig; 〉 Communicatie van het incident naar de getroffen gebruikers en eventueel VTC (volgens de criteria van VTC);

	〉 Uitvoeren van *lessons learned* na afsluiten van het incident en met verplicht verbetertraject via release management.
 	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Impact van het incident: hoge impact (want hoge materiële en/of lichamelijke schade mogelijk); 〉 Escalatie naar management van incidenten met prioriteit P1 of P2.
 	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Impact van het incident: hoge impact (want ernstige materiële en/of lichamelijk schade mogelijk).

Beschikbaarheid

Er zijn geen GDPR specifieke maatregelen gedefinieerd in het kader van beschikbaarheid.

1.3. Minimale specifieke (NIS II) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

1.4. Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van incidentbeheer toegepast worden:

Beschikbaarheid, Integriteit en Vertrouwelijkheid

IC klasse	Minimale maatregelen
  	Klasse 1, Klasse 2, Klasse 3, Klasse 4 en Klasse 5 kennen dezelfde maatregelen: 〉 Elke organisatie moet een systeem en formele, geactualiseerde procedures installeren die toelaten om veiligheidsinbreuken te detecteren, op te volgen en te herstellen in verhouding tot het technisch/operationeel risico (Ref. 5.9.7). 〉 Elke organisatie moet: ○ a. procedures hebben voor het vastleggen en beheren van incidenten over informatieveiligheid of privacy en de bijhorende verantwoordelijkheden. Deze procedures moeten bekend zijn bij alle medewerkers (Ref. 5.13.1 a).

 	○ b. Vastleggen in de overeenkomst met de medewerkers dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen (Ref. 5.13.1 b). ○ c. Gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen van de organisatie zodanig kenbaar maken dat de organisatie tijdig en adequaat corrigerende maatregelen kan nemen (Ref. 5.13.1 c). ○ d. Incidenten over informatieveiligheid en privacy zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO) rapporteren (Ref. 5.13.1 d). ○ e. Bij incidenten over informatieveiligheid of privacy het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzamelen (Ref. 5.13.1 e). ○ f. Elk incident over informatieveiligheid of privacy formeel evalueren opdat procedures en controlemaatregelen verbeterd kunnen worden. De lessen die getrokken worden uit een incident dienen gecommuniceerd te worden naar de directie van de organisatie voor validatie en goedkeuring van verdere acties (Ref. 5.13.1 f). ○ g. de 'richtlijn rond incidentenbeheer' toepassen zoals beschreven in de bijlage C van de beleidslijn 'incidentenbeheer' (Ref. 5.13.1 g). ○ KSZ bijlage C van de beleidslijn incidentenbeheer: ▪ Verantwoordelijkheid en procedures opstellen; ▪ Zwakheden rapporteren; ▪ Gebeurtenissen identificeren en rapporteren; ▪ Beoordeling van/beslissen over gebeurtenissen; ▪ Verzamelen en veilig stellen van bewijsmateriaal; ▪ Reageren op en herstellen van incidenten; ▪ Leren uit incidenten via rapport en evaluatie; ▪ Meldingen bij privacy incidenten.

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Beheer van incidenten als maatregel

2.1.1. Preventie, detectie en reactie

Maatregelen worden genomen als gevolg van een geïdentificeerd risico. Volgende mogelijkheden doen zich voor:

〉 **Preventie**: vermijden dat iets gebeurt of het verlagen van de waarschijnlijkheid dat het gebeurt;
〉 **Detectie**: detecteren van de (potentiële) schade zou een bedreiging optreden;
〉 **Reactie**: beperken van de schade wanneer een bedreiging optreedt of het effect hiervan gedeeltelijk of geheel corrigeren.

Bij preventieve maatregelen wordt de dreiging verkleint tot het niveau dat ze aanvaardbaar is.

Detectie maatregelen zorgen ervoor dat een dreiging en het gevolg ervan tijdig ontdekt wordt.

Reactieve maatregelen richten zich op de gevolgen indien een dreiging zich toch voordoet, door het inperken of herstellen van de schade.

Incident beheer is een reactieve maatregel.

2.1.2. De verschillende activiteiten van incident beheer

Een incident is een niet-geplande gebeurtenis in de dienstverlening of bedrijfsvoering waardoor de verwachte dienstverlening niet meer kan worden aangeboden of de bedrijfsvoering negatief beïnvloed wordt. In ITIL wordt een incident steeds behandeld in een helpdesk of service desk, maar soms beschikken organisaties enkel over een meldpunt of contact met ICT.

Incident beheer is het geheel van organisatorische en technische maatregelen dat ervoor zorgt dat een incident adequaat gedetecteerd, gemeld en behandeld wordt zodat de gevolgen voor de bedrijfsprocessen of schade ontstaan door het incident beperkt wordt tot een aanvaardbaar niveau.

Beheer van incidenten omvat:

- Registratie en categorisatie van het incident;
- Bepalen van de prioriteit (op basis van impact en urgentie);
- Behandelen van het incident (eventueel via doorverwijzing naar de nodige specialisten);
- Escalatie van het incident indien nodig;
- Documentatie van het incident;
- Afsluiten van het incident.

Incidenten worden aangereikt door gebruikers of door systeemwaarschuwingen, deze laatste zijn afkomstig uit het proces 'beheer van gebeurtenissen' (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen - beheer gebeurtenissen'*)

2.1.3. Behandelen van informatie veiligheidsincidenten

Voor de derde activiteit in incident beheer (behandelen van het incident) wordt in dit document de focus gelegd op het behandelen van informatie veiligheidsincidenten.

Behandelen van incidenten op het gebied van informatiebeveiliging omvatten de monitoring en detectie van informatie veiligheidsincidenten, maar ook het waarnemen van verdachte activiteiten door het personeel, en de uitvoering van de juiste acties als antwoord op deze gebeurtenissen.

Het proces dat ervoor zorgt dat informatie veiligheidsincidenten netjes worden afgehandeld omvat volgende stappen:

1) Identificatie en documentatie
2) Beperken van de schade
3) Remediatie
4) Herstel

5) Communicatie
6) Rapportering en evaluatie

Hoe groot of hoe klein het informatie veiligheidsincident ook is, deze stappen maken deel uit van het afhandelen van het incident. Voor een incident met beperkte impact worden deze stappen eerder intuïtief uitgevoerd, maar bij grote incidenten, d.w.z. met grote impact, waarbij meerdere personen betrokken zijn in de aanpak, ziet men een duidelijke uitvoering van de verschillende stappen.

Hoe groter het incident, hoe meer personen betrokken zullen zijn bij de aanpak om het incident onder controle te krijgen: een incident zal er dan toe leiden dat een incident team wordt samen geroepen. Ook de grootte van de organisatie speelt hierbij een rol: kleinere organisaties zijn vaak flexibel genoeg om het incident informeel in te dijken, waarbij de belijning van de verschillende stappen minder duidelijk is afgetekend.

De verschillende activiteiten worden toegelicht in het hoofdstuk: '*De bouwstenen van incident beheer*'.

2.1.4. Link met informatiebeveiliging

100% beveiliging bestaat niet. Incidenten kan men niet 100% voorkomen. (Informatie)veiligheidsincidenten zijn bijgevolg niet uit te sluiten. Het is dan ook zaak om de (informatie)veiligheidsdienst te betrekken bij de afhandeling van (informatie)veiligheidsincidenten.

In de praktijk betekent dit dat volgende functies deel uitmaken van het incident team:

- De CISO ingeval het incident gevolgen heeft voor de beveiliging van informatie en informatie verwerkende systemen;
- De DPO (indien deze functie bestaat in de organisatie) ingeval het incident gevolgen heeft voor de bescherming van persoonsgegevens;
- De safety manager ingeval het incident gevolgen heeft op de fysieke beveiliging en fysieke toegangscontrole.

Ook als het incident zelf geen rechtstreekse gevolgen heeft op de beveiliging van informatie en informatie verwerkende systemen, is het mogelijk dat bij de afhandeling van het incident wijzigingen nodig zijn aan de (ICT) infrastructuur. Hierbij moet de impact op de beveiliging steeds in het vizier worden genomen.

2.1.5. Link met risicoanalyse

Risico beheer om incidenten te voorkomen

Een risicoanalyse heeft als doelstelling inzicht te geven in de risicofactoren en welke impact en risico's deze met zich meebrengen. Dit inzicht helpt bij het nemen van maatregelen om risico's te beheersen. Deze maatregelen hebben betrekking op het beperken van de kans dat de gebeurtenis plaatsvindt en de impact van de risico's. Een goed inzicht in de risico's en de te nemen maatregelen om de risico's te beperken tot een aanvaardbaar niveau heeft ook een gunstig effect op incidenten: er zullen minder incidenten voorkomen en/of de gevolgen ervan zijn beperkt.

Incidenten als input voor risicoanalyses

Anderzijds kan de informatie uit incidenten gebruikt worden om de risicoanalyse effectiever te maken. Immers, deze incidenten geven reële informatie over de bedreigingen die zich hebben voorgedaan en de gevolgen hiervan op de dienstverlening/bedrijfsvoering. Informatie over incidenten over een langere periode kan aldus gebruikt worden om een juistere kwalificatie van de waarschijnlijkheid[1] van een bedreiging te bekomen.

Risicoanalyse tijdens incident beheer

Tot slot is het ook belangrijk om ervoor te zorgen dat risico's die verband houden met het incident worden gemitigeerd. Dit kan bijvoorbeeld door gevonden kwetsbaarheden weg te werken, toegangsrechten te herzien of niet toegelaten software te verwijderen.

2.1.6. Link met logging als maatregel

Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma's. Los van de detectie, wordt logging ook achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt waren. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet. Dan moet wel de integriteit van de logging goed ingericht zijn.

2.2. Succesfactoren voor een goed incident beheer

Om tot een efficiënt en effectief incident beheer te komen, zijn volgende parameters belangrijk. Zij kunnen meegenomen worden als prestatie-indicatoren of KPI's (zie hoofdstuk: *'Prestatie-indicatoren (KPI's)*') om het succes of falen van het proces te meten en bij te sturen waar nodig:

- **Tijdigheid**: een incident moet tijdig opgemerkt en aangepakt worden. Voorbeeld KPI: doorlooptijd vanaf aanname van een incident tot afsluiten van een incident, hoeveelheid afgehandelde incidenten per periode (bvb week, maand) t.o.v. het totaal aantal incidenten.
- **Volledigheid**: elk incident dat zich voordoet moet juist en volledig gedocumenteerd worden. Voorbeeld KPI: aantal niet geregistreerde incidenten, aantal onvolledig geregistreerde incidenten.
- **Beschikbaarheid** helpdesk/service desk: ondersteuning moet beschikbaar zijn voor gebruikers. Voorbeeld KPI: openingstijden helpdesk/service desk, wachttijden.
- **Juistheid**: een incident moet correct verholpen worden en de betrokkenen moeten correct geïnformeerd worden. Voorbeeld KPI: % de eerste maal correct verholpen incidenten, % van de verstoringen, waarbij de klant juist is geïnformeerd.
- **Deskundigheid**: er moet voldoende opgeleid personeel aanwezig zijn om incidenten vlot, correct en juist aan te pakken. Voorbeeld KPI: % functioneel geëscaleerde incidenten ten opzichte van het totaal aantal incidenten %, % hiërarchisch geëscaleerde incidenten ten opzichte van het totaal aantal incidenten %.
- **Klantvriendelijkheid**: dit is vooral belangrijk naar de ondersteuning van gebruikers. Voorbeeld KPI: aantal klachten over het functioneren van de helpdesk/service desk.

2.3. De bouwstenen van incident beheer

2.3.1. Registratie en categorisatie van het incident

Deze activiteit omvat de melding door een eindgebruiker aan de helpdesk of service desk, maar kan ook het gevolg zijn van detectie van incidenten door de ICT-beveiliging, doordat bij de controle van de logging iets naar boven komt of detectie door systeem/toepassingsmonitoring. In dit laatste scenario wordt de melding aangereikt vanuit het proces voor beheer van gebeurtenissen (‘event management’).

Het is belangrijk om elk incident zorgvuldig te registreren. Analoge incidenten kunnen later plaatsvinden en vereisen misschien dezelfde of analoge afhandeling. Een incident kan tevens onderdeel zijn van of aanleiding geven tot een ander of groter incident.

Het toewijzen van een categorie aan een incident laat toe om het incident vlot te documenteren en de informatie op te zoeken. Aan de hand van de categorie kan ook gezien worden of het een terugkerend incident is. Het opstellen van de verschillende categorieën vraagt de nodige aandacht. Vaak worden een aantal categorieën gedefinieerd, waarbij een categorie ‘overige’ wordt voorzien om alle incidenten op te vangen die niet in de gedefinieerde categorieën thuishoren. Het risico bestaat dan dat deze ‘overige’ uit gemakzucht wordt gebruikt waardoor de toegevoegde waarde van het toewijzen aan categorieën verdwijnt.

De categorisatie van een incident is belangrijk om de documentatie, opvolging en toewijzing te vergemakkelijken en om trends vast te stellen die bvb bij probleem beheer, beheer van providers enz. kunnen worden gebruikt.

2.3.2. Prioriteit bepalen van een incident

Het toewijzen van een prioriteit aan een incident geeft weer hoe ernstig en dringend een incident is en bepaalt de verdere afhandeling ervan. De prioriteit van een incident wordt bepaald door twee factoren:

〉 Impact: de omvang van het incident en de mogelijke schade als gevolg van het incident
〉 Urgentie: de maat voor hoe snel een incident moet worden afgehandeld

Voor de inschatting van de urgentie van een incident worden schalen gehanteerd van laag naar hoog, waarbij de inschatting bepaald wordt door:

〉 De snelheid waarmee de schade toeneemt,
〉 Het type gebruikers of systemen dat getroffen is,
〉 Het aantal gebruikers of systemen dat getroffen is,
〉 De hoeveelheid werk om de schade te herstellen,
〉 De mogelijkheid om een groter incident als gevolg van het incident te voorkomen.

Urgentie	**Omschrijving**
Hoog	• Geen controle op oorzaak noch gevolgen • Controle op oorzaak maar niet op gevolgen • Schade veroorzaakt door het incident neemt snel toe • Werk dat moet worden hersteld door medewerkers is zeer arbeidsintensief • Voorkomen dat incident leidt tot een groot incident door snel op te treden
Medium	• Geen controle op oorzaak maar gevolgen zijn onder controle • Schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe • Er gaat werk verloren maar dit is relatief snel te herstellen
Laag	• Oorzaak en gevolgen zijn onder controle • Schade veroorzaakt door het incident neemt in de tijd weinig toe • Het werk dat blijft liggen is niet arbeidsintensief

Voor de inschatting van de impact worden eveneens schalen gehanteerd van laag naar hoog, bepaald door:

1) Schade of impact voor de organisatie:
   〉 Het aantal mensen dat geïmpacteerd is (hoeveel gebruikers, hoeveel afdelingen zijn getroffen),
   〉 Het aantal betrokkenen dat geïmpacteerd is,
   〉 Grootte van de financiële impact,
   〉 Grootte van de lichamelijke schade,
   〉 Mogelijke reputatieschade.

2) Wanneer het incident persoonsgegevens betreft, wordt de impact bovendien gerelateerd aan:
   〉 De aard en de omvang van de inbreuk,
   〉 De aard van de getroffen persoonsgegevens,
   〉 De mate waarin technische maatregelen getroffen zijn ter bescherming van de getroffen persoonsgegevens,

〉 De gevolgen voor de persoonlijke levenssfeer van de betrokkenen.

Impact	Omschrijving
Hoog	• Ernstige of bedreigende schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Lange onderbreking of permanente onbeschikbaarheid van de dienstverlening is mogelijk • Hoge financiële impact • Hoge reputatieschade • Ernstige materiële of lichamelijke schade voor individuen
Medium	• Belangrijke schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Korte onderbreking van de dienstverlening is mogelijk • Matige financiële impact • Matige reputatieschade • Matige materiële schade voor individuen
Laag	• Geen of minimale schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Dienstverlening gegarandeerd of slechts kort onderbroken • Geen of beperkte financiële impact • Geen of beperkte reputatieschade • Geen of beperkte materiële schade voor individuen

Impact en urgentie worden tegen mekaar afgezet om de prioriteit te bepalen, wat wordt weergegeven in een prioriteiten matrix:

		Impact		
		Hoog	Medium	Laag
Urgentie	Hoog	**Blokkerend** (P1)	**Ernstige storing** (P2)	**Matig storend** (P3)
	Medium	**Ernstige storing** (P2)	**Matig storend** (P3)	**Niet storend** (P4)
	Laag	**Matig storend** (P3)	**Niet storend** (P4)	**Niet storend** (P4)

Indicatoren de prioriteit van een incident kunnen beïnvloeden, zijn:

〉 Bedrijfskritische toepassingen of processen zijn betrokken bij het incident,
〉 Bedrijfskritische personen zijn getroffen.

De verwachte doorlooptijd voor de afhandeling van een incident hangt af van de prioriteit die aan het incident werd toegekend:

Prioriteit	**Maximale reactietijd**	**Maximale oplossingtijd**
P1 = blokkerend	½ uur	24 uur
P2 = ernstige storing	1 uur	72 uur
P3 = matig storend	4 uur	1 week
P4 = niet storend	8 uur	1 maand

Reactietijd: tijd tussen aanmelden en eerste reactie;

Oplossingtijd: tijd tussen aanmelden en oplossen of inperken van het incident.

Het vaststellen van de prioriteit van een incident is geen statisch of eenmalig gegeven: het is mogelijk dat gedurende de levensloop van een incident de prioriteit wijzigt, bvb omdat meer informatie ter beschikking komt of omdat de gevolgen van een incident veranderen. Een op zich staand klein incident kan bovendien de voorbode zijn van een groter of complexer incident. Zo zal een incident gemeld door één gebruiker waarschijnlijk geen hoge prioriteit krijgen, maar dat verandert snel zodra meerdere gebruikers een gelijkaardige melding plegen.

Wanneer beroep gedaan wordt op externe dienstverlening, is een prioriteiten matrix vaak al vastgelegd door de dienstverlener. Het volstaat dan om eenvoudig bovenstaande matrix te mappen op de matrix van de dienstverlener.

2.3.3. Behandelen van het incident

We beperken ons tot de bouwstenen nodig voor het afhandelen van informatie veiligheidsincidenten.

Beperken van de schade

In deze stap wordt verdere schade als gevolg van het incident zoveel mogelijk ingeperkt. Een verdere, grondige beoordeling van de aard en omvang van het incident dringt zich op. Er moet vastgesteld worden wat de schade is en eventueel bewijsmateriaal moet veiliggesteld worden. Indien het een verwerking van persoonsgegevens betreft, moet bepaald worden of er een inbreuk heeft plaats gevonden dat onder de meldplicht AVG valt.

Er worden tevens maatregelen genomen om de oorzaak van het incident te blokkeren of te verwijderen, de impact te verminderen door verdere blootstelling aan de oorzaak van het incident te voorkomen.

Vaak wordt een team toegewezen aan het incident – het incident team. Dit team is belast met het vaststellen van de schade en een grondige beoordeling van de aard en omvang van het incident. Ook hier speelt de grootte van de organisatie een rol: kleine(re) organisaties hebben vaak geen ‘echt’

incident team, maar leunt op de verschillende medewerkers om het incident aan te pakken en de schade te beperken.

Een belangrijke actie is tevens het veiligstellen van bewijsmateriaal dat kan dienen ingeval het incident het gevolg is van een inbraak poging. Voorbeelden van zo'n bewijsmateriaal zijn:

- Images van disks,
- Netwerkverkeergegevens van en naar de gecompromitteerde apparatuur,
- Log bestanden van toepassingen, systemen en toegangslogs.

Een incident onder controle krijgen betekent dus het beperken van de schade, het verhinderen dat andere systemen hinder ondervinden van het incident en het eventuele stoppen van een aanval. Zo kan een toepassing van het internet afgeschakeld worden om te voorkomen dat een cyberaanval zich voortzet. Er moet verhinderd worden dat het incident zich uitbreidt, zowel binnen de organisatie als buiten de organisatie (derde partijen waarmee de ICT-systemen geconnecteerd zijn). In sommige gevallen is het zelfs niet mogelijk om de normale activiteiten van de organisatie onmiddellijk te hernemen. In dit geval zal getracht worden om zo snel mogelijk de basisfunctionaliteiten te laten functioneren en ervoor te zorgen dat (een deel van) de bevoegde gebruikers hun toegang behouden.

Remediatie

Remediatie is een belangrijke stap in het beheersen van een incident. Remediatie houdt in dat de oorzaak van het incident geblokkeerd of weggenomen wordt. Voorbeelden van remediatie zijn: services of processen stoppen, corrupte toepassingen verwijderen, computers opnieuw opstarten, gebruikersaccounts uitschakelen, netwerkverbindingen sluiten, caches flushen.

Het wegnemen van de oorzaak van een incident kan vele vormen aannemen, bvb:

- Een virus- of spywarescanner gebruiken om de kwaadaardige bestanden en services te verwijderen;
- Handtekeningen bijwerken;
- Malware verwijderen;
- Aangetaste gebruikersaccounts uitschakelen;
- Wachtwoorden van aangetaste gebruikersaccounts wijzigen;
- Alle uitgebuite kwetsbaarheden identificeren en verhelpen;
- Gaten in de veiligheid identificeren en herstellen.

Herstel

In deze fase wordt het systeem/de systemen hersteld zodat de bedrijfsprocessen en -functies terugkeren naar de normale werking. Vaak zijn er verschillende opties om te herstellen na een incident en moet er bekeken worden welke de beste keuze is op gebied van hersteltijd, kostprijs en herstel of beperking van potentieel gegevensverlies.

Wanneer een systeem of systemen opnieuw moeten worden heropgebouwd, is het aspect beveiliging belangrijk: vooraleer het systeem opnieuw in gebruik wordt genomen, moet het worden goedgekeurd op niveau beveiliging.

Communicatie

Communicatie is een belangrijke stap in het incident beheersproces: dit betekent controle houden over de informatiestroom en ervoor zorgen dat geautoriseerde personen de juiste informatie op het juiste moment bij de juiste belanghebbenden bezorgen. Het gaat zowel over interne als over externe communicatie.

Als er een inbreuk is waarbij melding aan de GBA (Gegevensbeschermingsautoriteit) verplicht is, dan is de eerste melding al gebeurd. Op basis van het detailonderzoek kan nu de volledige melding voorbereid en uitgevoerd worden. Als nu pas blijkt dat er een meldplicht is voor een inbreuk, dan moet de volledige melding gedaan worden (als de wettelijke termijn van 72 uur overschreden is, dan moet dat worden gemotiveerd). Indien noodzakelijk moeten andere overheidsinstanties op de hoogte worden gebracht.

Communicatie naar eindgebruikers, en eventueel externe communicatie naar vb. pers en media kan ook een noodzakelijke stap zijn.

Het type incident en de (mogelijke) gevolgen ervan bepalen het type communicatie en het tijdsstip van communiceren dat nodig is. Daarom is het belangrijk om vooraf de verschillende belanghebbenden te identificeren:

Belanghebbenden	**Informatie**
Directie	Welke activiteiten zijn getroffen? Wat zijn de gevolgen? Wanneer is de situatie terug normaal?
Betrokken bedrijfsmanagers	Wanneer is de situatie terug normaal?
Werknemers	Wat wordt van hen verwacht? Wanneer is de situatie terug normaal?
Media	Indien het incident voor de buitenwereld zichtbaar is: officiële verklaring over het incident en impact.
Gebruikers	Zijn er gevolgen voor gebruikers (intern, extern)? Zijn er persoonsgegevens betrokken bij het incident?
Leveranciers	Kan het incident gevolgen hebben voor (sommige) leveranciers? Moeten zij maatregelen nemen om een potentiële impact te mitigeren?
Andere incident teams	Communicatie met andere incident teams voor technische ondersteuning.
Internet serviceprovider	Voor ondersteuning ingeval van een internet-gerelateerd incident (hacking).
GBA/VTC	Wettelijke meldplicht ingeval persoonsgegevens betrokken zijn bij het incident.

CERT.be	Technische gegevens en bewijsmateriaal ingeval van een cyber security incident.
Politie	Is er een vermoeden van crimineel opzet?

Bij het opzetten van een communicatieplan voor het incident moet er rekening worden gehouden met het verstrekken van regelmatige updates over het incident.

Afhankelijk van de gevolgen van het incident moet het communicatieplan verschillende doelstellingen dienen:

- Communicatie om het incident aan te pakken en op te lossen;
- Communicatie gericht op compliance, dit omvat communicatie naar getroffen gebruikers en aan toezichthouders;
- Communicatie om imagoschade te beperken, dit omvat communicatie met getroffen gebruikers, partners, media en werknemers.

Meestal worden verschillende communicatiekanalen gebruikt:

- E-mail,
- Website (intern en publiek),
- Sociale media,
- Telefonisch,
- Tijdens overlegmomenten,
- Op papier (mededelingen op borden en deuren, overhandigd bij toegangspunten, …).

Rapportering en evaluatie

Het is nodig om relevante informatie te rapporteren aan belanghebbenden zoals o.a. (top)management (directie, raad van bestuur) en de informatieveiligheidsdienst (CISO, DPO, …). De doelgroep voor de rapportage is afhankelijk van organisatie tot organisatie en wordt best vooraf vastgelegd.

Grote veiligheidsincidenten moeten onmiddellijk aan het management worden gerapporteerd. Het is ook raadzaam periodiek de veiligheidsincidenten toe te lichten aan de mensen binnen de organisatie belast met het in kaart brengen van de risico's voor de organisatie.

Het kan noodzakelijk zijn om na een incident een evaluatie te maken van het incident, de ondernomen stappen en hoe dit incident in de toekomst kan worden vermeden, deze stap wordt ook *lessons learned* genoemd. Het resultaat van dergelijke analyse kan aanleiding geven tot een verbetervoorstel met volgende kenmerken:

- Een geplande wijziging: er kan geoordeeld worden dat een specifieke actie nodig is binnen een aanvaardbare termijn, deze wordt opgenomen via het proces wijzigingsbeheer;
- Een niet-geplande wijziging: het betreft een verbetervoorstel waarvan de implementatie datum niet onmiddellijk kan worden opgesteld, deze wordt opgenomen via het proces beheer van releases.

2.3.4. Escalatie

Incidenten komen meestal op een min of meer centrale plaats terecht: vaak is dit een service desk, maar in organisaties waar deze functionaliteit ontbreekt, zijn er vaak één of meerdere personen aangeduid waar gebruikers terecht kunnen met hun ICT-problemen en/of is er een ICT-team dat zich buigt over door systemen gegenereerde waarschuwingen.

In eerste instantie zal de (servicedesk) medewerker controleren of een vergelijkbaar incident eerder is voorgekomen en of er een oplossing of *work around* voorhanden is. Sommige incidenten hebben echter geen voor de hand liggende oplossing of vragen meer expertise. Deze incidenten worden dan doorverwezen naar iemand met meer kennis of meer beslissingsbevoegdheid: het incident wordt dan geëscaleerd. Bij escalatie maakt men onderscheid tussen functionele en hiërarchische escalatie:

- **Functionele escalatie**: doorverwijzing naar iemand met meer kennis, ook wel horizontale escalatie genoemd;
- **Hiërarchische escalatie**: doorverwijzing naar iemand met meer bevoegdheden, ook wel verticale escalatie genoemd.

Voor functionele escalatie gelden criteria zoals kennis en ervaring. Er wordt vaak ook gesproken over eerstelijnssupport (service desk), tweedelijnssupport en (gespecialiseerde teams) en zelfs derdelijns support (leveranciers).

Gedurende het traject wordt het incident record voortdurend bijgewerkt door de medewerkers die aan het incident werken.

Wanneer er geen oplossing voor het incident voorhanden is, wordt het doorverwezen naar het proces probleem beheer (voor meer informatie zie document *'Vo Informatieclassificatie - Minimale maatregelen - probleem beheer'*)

2.3.5. Documentatie van het incident

Het is belangrijk om elk incident en de ondernomen acties te documenteren en al deze informatie bij te houden. Hoe incidenten worden gedocumenteerd, hangt af van de grootte van de organisatie: voor grote organisaties, (ICT) providers en dienstenleveranciers met een professionele helpdesk/service desk is een geautomatiseerde opvolgingstool onontbeerlijk. Voor kleine organisaties kan het volstaan om de incidenten te registreren in een eenvoudig logboek.

Er is ook de wettelijke verplichting tot het bijhouden van een register van incidenten rond persoonsgegevens wanneer de organisatie persoonsgegevens verwerkt (noteer dat elke organisatie minstens de gegevens van haar werknemers verwerkt – een organisatie vinden die geen persoonsgegevens verwerkt, is dus een moeilijke opgave).

Het documenteren van informatie over incidenten moet op een gestandaardiseerde manier verlopen, om te verzekeren dat het efficiënt en effectief gebeurt.

Voor niet geautomatiseerde meldingen van gebeurtenissen moeten minstens volgende elementen bijgehouden worden:

- Wat was de gebeurtenis?
- Wie heeft de feiten vastgesteld?
- Wanneer heeft de gebeurtenis plaatsgevonden?
- Wanneer werden de feiten vastgesteld?
- Hoe werd de gebeurtenis veroorzaakt?
- Hoe werden de feiten vastgesteld?

- Wat heeft de gebeurtenis beïnvloed?
- De (potentiële) impact van de gebeurtenis op de activiteiten van de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces

Incidenten worden best gedocumenteerd, inclusief datum en tijd, in incident records, waarbij elk record slaat op één enkel incident. Dit geldt zowel voor incidenten die zijn gemeld door personen, als voor incidenten die automatisch zijn opgespoord via systeem event waarschuwingen. Documenteer alle relevante informatie over de aard van het incident zodat een volledig en historisch record ontstaat. Als het incident dan moet worden overgedragen naar andere (support) groepen, hebben ze alle nodige informatie ter beschikking. Een incident record omvat:

- Een uniek referentienummer;
- Incident categorie;
- Incident prioriteit (op basis van urgentie en impact);
- Naam van de persoon of afdeling die het incident heeft geregistreerd;
- Beschrijving van het incident;
- Ondernomen activiteiten;
- Status van het incident;
- Aan wie het incident werd overgedragen.

Software kan de registratie van incidenten helpen en gedeeltelijk automatiseren. Dit gebeurt in (incident) ticketing systemen. Essentiële functies van zo'n ticketing systeem zijn:

- Workflow beheer;
- Alerts beheren en escaleren;
- Automatische routing;
- Contract en SLA beheer.

Merk op dat niet alleen incidenten in zo'n ticketing systeem worden geregistreerd, maar ook service aanvragen en aanvragen voor informatie.

Het is ook belangrijk om de laatst bekende informatie van het incident goed bij te houden en te registreren: de prioriteit kan bvb in de loop van de afhandeling wijzigen, het incident kan toegewezen worden aan een andere supportgroep, de status van het incident wijzigt in de loop van de afhandeling enz. Deze nieuwe informatie moet toegevoegd worden aan het incident record zodat het record op elk moment de laatste bekende informatie over het incident bevat.

2.3.6. Helpdesk/service desk

Een **helpdesk** is bedoeld om de klant of interne gebruiker van informatie en ondersteuning te voorzien met betrekking tot bedrijfsprocessen, producten en diensten. Het doel van een helpdesk is om een centrale bron van antwoorden te zijn, problemen op te lossen en bekende problemen te helpen oplossen. Helpdesk support kan langs verschillende kanalen aangeboden worden, waaronder fysieke locaties, gratis telefoonnummers, websites, instant messaging of e-mail. Een helpdesk kan deel uitmaken van een service desk.

De primaire rol van de helpdesk bestaat uit:

- Optreden als SPOC (Single Point of Contact) voor gebruikers;
- Registratie, documentatie en opvolging van incidenten;
- Routeren van incidenten (functionele en hiërarchische escalatie);
- Eerstelijnssupport voor oplossen van incidenten.

De primaire rol van een **IT-service desk** is om als centraal contactpunt te dienen voor het controleren/beheren van incidenten, het behandelen van de (aan)vragen van gebruikers en als communicatiekanaal tussen verscheidene service managementfuncties en de gebruikers. Daarnaast speelt de service desk vaak een actieve rol bij het ontdekken van veranderingsverzoeken, contact met ondersteuningscontracten van derden, het management van software licenties en assistentie bij probleemmanagement.

De primaire rol van een service desk is:

- Optreden als SPOC (Single Point of Contact) voor alle bedrijfsprocessen;
- Integratie met andere processen zoals wijzigingsbeheer, configuratiebeheer, release management en probleembeheer;
- Ondersteunt conformiteit met Service Level Management contracten;
- Ondersteunt de service cataloog.

Het grote verschil tussen een service desk en een helpdesk, is dus dat de helpdesk een probleem meestal alleen registreert, oplost (aan de hand van gekende oplossing of *work around*) of doorstuurt naar een tweede lijn. Bij een service desk ligt de dienstverlening hoger. Op een service desk worden bijvoorbeeld ook autorisaties verleend en ICT-gerelateerde bestellingen aangenomen.

Zowel helpdesk als service desk kunnen intern opgenomen worden of uitbesteed aan dienstenleverancier.

2.3.7. Het incident team

Wanneer een incident van enige omvang de organisatie teistert, is vaak een team van specialisten nodig om het incident aan te pakken. Er moeten immer activiteiten vanuit verschillende invalshoeken opgestart worden om een antwoord te bieden op een aantal vragen zoals:

- Wie beantwoordt de interne vragen rondom incidenten?
- Welke taken moeten opgestart worden? Wie is verantwoordelijk voor deze taken?
- Wie beheert het incident aan de technische kant?
- Wie heeft beslissingsbevoegdheid?
- Wie onderhoudt het contact met de directie/raad van bestuur?
- Wie kan de externe partners contacteren?
- Wie kan de betrokken leveranciers en dienstenleveranciers contacteren?
- Wie kan een klacht indienen bij de autoriteiten en toezichthouders?
- Wie is belast met de communicatie met externen zoals pers, hulpdiensten, gebruikers?

Aangezien het hier om een diverse samenstelling van profielen gaat, is het logisch dat een team van personen samen het incident aanpakken. Voor een kleine organisatie zal het team eerder beperkt zijn en de communicatielijnen kort.

Om een incident van enige omvang aan te pakken, zijn er dus verschillende vaardigheden nodig om de verschillende verantwoordelijkheden en activiteiten op te nemen om op efficiënte wijze op het incident te reageren:

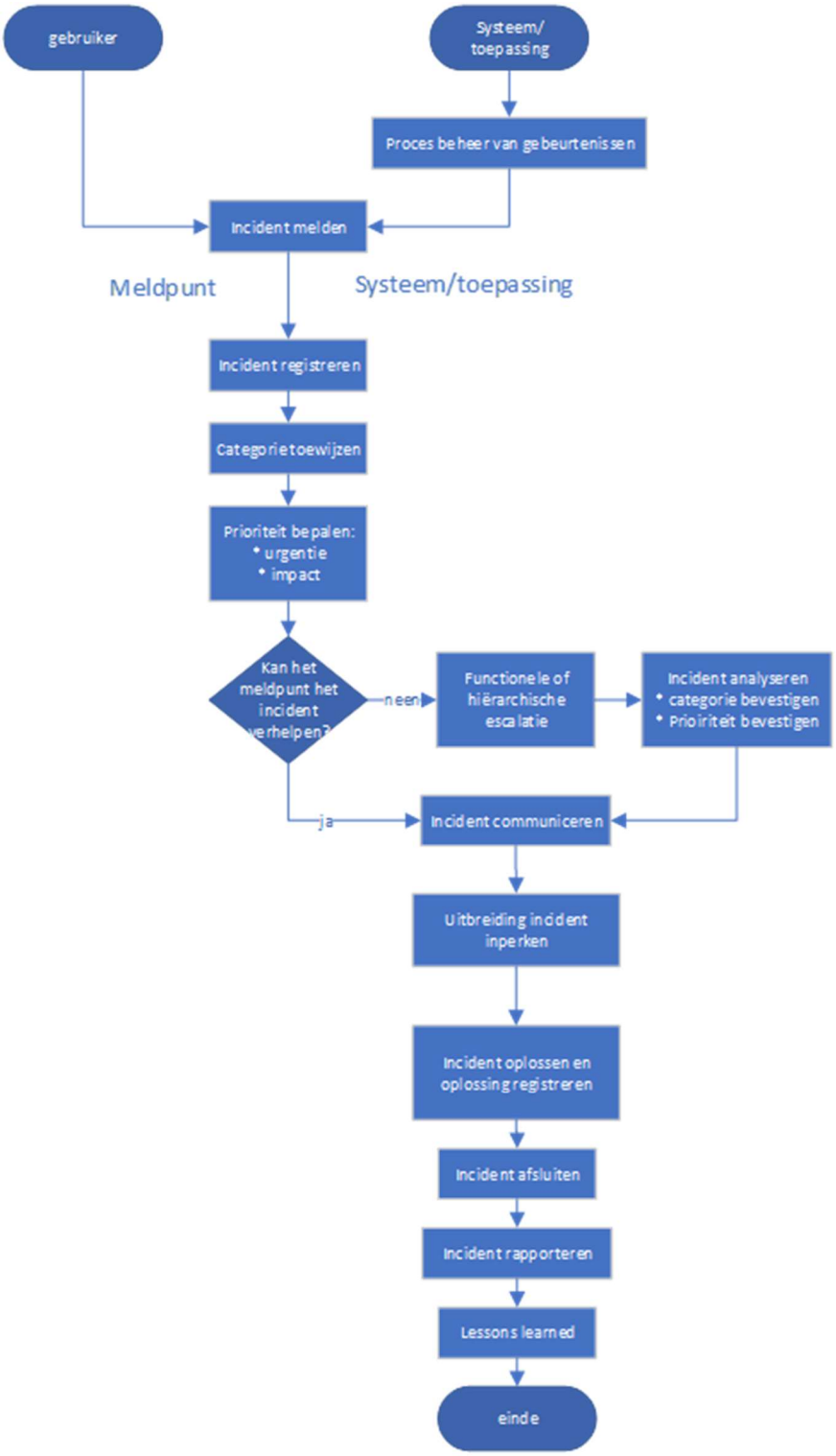
Vaardigheden	**Verantwoordelijkheden**	**Functie**
Incidentbeheer	Beheer van het incident vanaf detectie tot afsluiting.	Incident manager
Bevoegdheid om zakelijke beslissingen te nemen	De impact op de organisatie beoordelen en als dusdanig handelen. Beslissingen nemen over hoe verder te gaan. Beslissen wanneer herstelactiviteiten worden opgestart. Beslissen of een klacht wordt ingediend.	Management
Netwerkbeheer	Technische kennis over het netwerk. De gegevensstroom van en naar het netwerk analyseren en eventueel blokkeren. Informatiebeveiliging op niveau IT en IT-continuïteit.	ICT-personeel voor technische ondersteuning
Beheer van gebruikersapparatuur en servers	Aangetaste gebruikersapparatuur en servers analyseren en beheren.	ICT-personeel voor technische ondersteuning
Beheer van toepassingen	Niet of slecht functionerende toepassingen onder de loep nemen. Ervoor zorgen dat toepassingen al dan niet gedeeltelijk aan de gebruikers worden ter beschikking gesteld na het incident.	ICT-personeel voor technische ondersteuning
Juridisch advies	De contractuele en juridische impact van een incident beoordelen. Verzekeren dat incident	Juridische afdeling/ bedrijfsjurist

	response activiteiten binnen wettelijke en regelgevende beleidsgrenzen blijven.	
Communicatie	Op een gepaste manier communiceren naar alle belanghebbenden: klanten, aandeelhouders, personeel. Communicatie naar de pers.	Communicatie of pr-afdeling
Forensische vaardigheden	Op een gepaste manier bewijzen verzamelen, analyseren en vrijwaren (zodat het bewijs eventueel door een rechtbank wordt aanvaard).	ICT-personeel voor technische ondersteuning
Fysieke veiligheid	De aspecten van het incident behandelen die gekoppeld zijn aan fysieke toegang en fysieke beveiliging.	Safety manager
Crisisbeheer	Indien het incident geëscaleerd wordt naar een crisis.	Crisismanager

De grootte van de organisatie bepaalt of en hoeveel functies er nodig zijn. Kleinere organisaties hebben vaak de flexibiliteit om zich voor de aanpak van het incident snel tot het management te wenden. Dit is niet het geval voor grotere organisaties. Daar zal het incident team de meeste incidenten op een meer autonome wijze behandelen, zodat de bedrijfstop alleen in geval van een bijzonder ernstig incident wordt betrokken. Hoe groter de organisatie, hoe gedifferentieerder de samenstelling van het incident team moet zijn. In grotere organisaties kan er naast een incident team ook een crisisteam worden samengesteld uit vertegenwoordigers van het ondernemingsbestuur die bij ernstige incidenten de verantwoordelijkheid opnemen voor de strategische en bedrijfsbeslissingen en de communicatie hierover. Op deze manier kan de incident manager zich meer richten op de technische kwesties van het incident. Kleinere organisaties zullen ook vaker beroep doen op externe experts, bvb voor forensisch onderzoek of juridische ondersteuning.

2.3.8. Het proces

Alle bouwstenen samen maken deel uit van het proces voor het beheer van incidenten. Algemeen ziet dat er als volgt uit:



3. LINK MET ANDERE MAATREGELEN

Beheer van incidenten is geen alleenstaand proces maar heeft interacties met de andere beheersprocessen:

〉 **Beheer van gebeurtenissen** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – beheer gebeurtenissen')

Er is een directe link met beheer van gebeurtenissen aangezien alle problemen aangeleverd worden door dit proces.

〉 **Probleembeheer** (voor meer informatie zie document: Vo Informatieclassificatie - Minimale maatregelen – probleem beheer')

Er is een directe link met probleem beheer aangezien alle problemen aangeleverd worden door dit proces.

〉 **Wijzigingsbeheer** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer')

Er is een directe link met wijzigingsbeheer aangezien alle problemen aangeleverd worden door dit proces.
Om een gekende fout te herstellen en dus de oorzaak van één of meerdere incidenten structureel weg te werken, dient vaak een wijziging uitgevoerd te worden. Indien het gaat om een in te plannen wijziging, wordt dit opgenomen door wijzigingsbeheer.

〉 **Configuratie beheer** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer')

Dit proces levert informatie over de betrokken configuratie-items aan probleembeheer. De informatie die de Eigenaar moet bijhouden is de classificatie op gebied van Vertrouwelijkheid, Integriteit en Beschikbaarheid.

〉 **Continuiteitsbeheer** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen - incident beheer')

Er is een directe link met incident beheer aangezien alle problemen aangeleverd worden door dit proces.

〉 **Release en deployment beheer** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen - release en deployment')

Indien het gaat om een niet-geplande wijziging, dient dit opgenomen te worden door dit proces.

4. PRESTATIE-INDICATOREN (KPI'S)

Om de efficiëntie en effectiviteit van een proces te kwalificeren en waar nodig bij te sturen wordt een proces gemeten aan de hand van prestatie-indicatoren. De belangrijkste indicatoren worden KPI's of Key Performance Indicatoren genoemd. Per KPI wordt een norm afgesproken en de rapportering gebeurt per periode, bvb maandelijks of halfjaarlijks.

KPI's worden ook gebruikt om bij outsourcing en externe dienstverlening de kwaliteit van het uitbestede proces op te volgen. Deze KPI's worden dan ook vaak opgenomen in de SLA.

Voorbeelden van KPI's voor het proces incident beheer zijn:

- Aantal incidenten per maand;
- Aantal openstaande incidenten per maand;
- Aantal opgeloste incidenten per maand;
- Doorlooptijd van een incident (van melding tot afsluiting);
- Aantal informatie veiligheidsincidenten t.o.v. het totaal aantal incidenten;
- Aantal niet geregistreerde of onvolledige incidenten;
- Openingstijden helpdesk;
- Wachttijden;
- Aantal incidenten dat bij eerste melding correct verholpen is;
- Aantal incidenten met juist communicatie naar betrokkenen;
- Aantal geëscaleerde incidenten (functioneel en hiërarchisch);
- Aantal klachten over de helpdesk.

Het vastleggen van de juiste prestatie-indicatoren is een moeilijke klus die de nodige aandacht vraagt: een teveel aan KPI's zal de organisatie (te) veel werk bezorgen, maar te weinig of onjuiste KPI's schetsen geen goed beeld van de kwaliteit van het incident beheerproces.

De doelgroep voor de rapportering bepaalt tevens het type KPI: zo zal de incident manager of CISO belang stellen in andere prestatie-indicatoren dan bvb de directie.