Informatieclassificatie Vlaamse overheid (Vo-ICR)

Beheer van gebeurtenissen (event management)

Minimale maatregelen

Team Informatieveiligheid | Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

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 op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

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

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 Vlaamse overheid 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	22 juli 2019	Kristel VAN AKEN	Draft
v.0.2	20 augustus 2019	Kristel VAN AKEN	Feedback taakgroep
v.0.3	12 december 2019	Kristel VAN AKEN	Feedback leespanel en consistentie check
v.1.0	12 december 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.1.3.	10 augustus 2021	Beau JANSSEN	Toevoeging Beschikbaarheid als kwaliteitskenmerk
v.2.0	22 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 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 - incident beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – SIEM*
  - *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 'beheer van gebeurtenissen' (*event management*)

Het beheer van gebeurtenissen is de basis voor de monitoring, opvolging en controle van ICT.

Het doel van dit proces is de registratie en afhandeling van gebeurtenissen, die waargenomen, geprioriteerd en getypeerd werden op het bronproces (toepassing of systeem). Daar het quasi onmogelijk is om alle gebeurtenissen te detecteren en op te volgen, is het belangrijk om een juiste set uit te selecteren met volgende kenmerken:

- De gebeurtenis moet detecteerbaar zijn a.d.h.v. monitoring- of systeem tools,
- De gebeurtenis moet relevant zijn om de zakelijke of ICT-processen te behoeden van degradatie, uitval of verstoring,
- Het moet mogelijk zijn om acties te definiëren als antwoord op een gebeurtenis die als waarschuwing of uitzondering getypeerd is.

Event management of beheer van gebeurtenissen is dus het bewaken van alle significante events (gebeurtenissen) die geautomatiseerd kunnen worden en die plaatsvinden in de ICT-infrastructuur om de normale uitvoering te monitoren en onvoorziene omstandigheden op te sporen en te escaleren. De identificatie van de te bewaken gebeurtenissen van het bron proces is dan ook onontbeerlijk voor het proces 'beheer van gebeurtenissen', maar maakt geen deel uit van dit proces (het bron proces moet deze identificatie op zich nemen).

Het bron proces levert dus input aan het proces beheer van gebeurtenissen met volgende attributen:

- De criticiteit van het bron proces,
- De gebeurtenissen gegenereerd door het bron proces,
- De typering van de gebeurtenis (informationele gebeurtenis, waarschuwing, uitzondering).

Event management houdt het beheer in van 2 soorten gebeurtenissen:

- De gebeurtenissen gegenereerd door het bron proces,
- Opvolgen van de beschikbaarheid en integriteit van deze gebeurtenissen: erover waken dat de gebeurtenissen gegenereerd door het bron proces opgepikt worden door het proces 'event management' en erover waken dat de gebeurtenis wel degelijk door het beoogde bron proces werd gegenereerd.

1. MINIMALE MAATREGELEN

Het beheren van gebeurtenissen 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 beheer van gebeurtenissen*'):

- Registratie van een gebeurtenis in event management;
- Filteren van gebeurtenissen;
- Correlatie toepassen;
- Reageren op gebeurtenissen.

Daarnaast moet ook rekening worden gehouden met:

- De soorten gebeurtenissen opgevolgd in event management;
- De typering van de gebeurtenis;
- Review acties door het bron proces.

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

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen

	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	
	- Registratie van gebeurtenissen:
	- Over confidentialiteit, integriteit en beschikbaarheid van het bron proces;
	- Over beschikbaarheid en integriteit van de gebeurtenissen uit het bron proces.
	  - Filteren van gebeurtenissen;
	  - Correlatie toepassen;
	- Reageren op gebeurtenissen:
	  - Logging van gebeurtenissen;
	  - Notificatie uitsturen bij waarschuwingen en uitzonderingen;
	  - Auto response;
	  - Incident aanmaken bij uitzonderingen (altijd);
	  - Incident aanmaken bij waarschuwingen indien nodig.
	- De soorten gebeurtenissen opgevolgd in het proces:
	  - Falen;
	  - Fouten;
	  - Overschrijding drempelwaarden;
	  - Niet-geoorloofde creaties, wijzigingen en verwijderingen;
	  - Aanwezigheid van informatieklasse 3 of hoger;
	  - Beschikbaarheid en integriteit van de gebeurtenis.
	- De typering van de gebeurtenis: waarschuwingen en uitzonderingen.

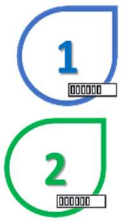
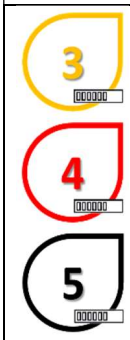
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Aanwezigheid van informatie van een hogere klasse. 〉 Review acties door het bron proces.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Succes en falen; 〉 De typering van de gebeurtenis: informationele gebeurtenis, waarschuwingen en uitzonderingen.

Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Registratie van gebeurtenissen: 〉 Over confidentialiteit, integriteit en beschikbaarheid van het bron proces; 〉 Over beschikbaarheid en integriteit van de gebeurtenissen uit het bron proces. 〉 Filteren van gebeurtenissen; 〉 Correlatie toepassen; 〉 Reageren op gebeurtenissen: 〉 Logging van gebeurtenissen; 〉 Notificatie uitsturen bij waarschuwingen en uitzonderingen; 〉 Auto response; 〉 Incident aanmaken bij uitzonderingen (altijd); 〉 Incident aanmaken bij waarschuwingen indien nodig. 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Falen; 〉 Fouten; 〉 Overschrijding drempelwaarden; 〉 Niet-geoorloofde creaties, wijzigingen en verwijderingen; 〉 Aanwezigheid van informatieklasse 3 of hoger; 〉 Beschikbaarheid en integriteit van de gebeurtenis. 〉 De typering van de gebeurtenis: waarschuwingen en uitzonderingen.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Aanwezigheid van informatie van een hogere klasse. 〉 Review acties door het bron proces.

	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Succes en falen; 〉 De typering van de gebeurtenis: informationele gebeurtenis, waarschuwingen en uitzonderingen.

Beschikbaarheid

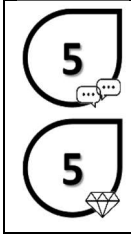
IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces wijzigingsbeheer is minimaal kantooruren (5d x 10u) 〉 Registratie van gebeurtenissen: 〉 Over confidentialiteit, integriteit en beschikbaarheid van het bron proces; 〉 Over beschikbaarheid en integriteit van de gebeurtenissen uit het bron proces.
	Klasse 3 en Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Beschikbaarheid van het proces wijzigingsbeheer is minimaal kantooruren (24u x 7d)

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor beheer gebeurtenissen 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 maatregelen voor klasse 1 en Klasse 2.
	Maatregelen voor Klasse 4: 〉 De soorten gebeurtenissen opgevolgd in het proces: 〉 Succes en falen.
	Er zijn geen GDPR maatregelen voor klasse 5.

Beschikbaarheid

Er zijn geen GDPR maatregelen voor beschikbaarheid.

1.3 Minimale specifieke (NISII) 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

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

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

Beschikbaarheid, Integriteit en vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 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. KSZ 5.13.1).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1 Beheer van gebeurtenissen als maatregel

2.1.1 Preventie, detectie en reactie

Het proces beheer van gebeurtenissen of *event management* laat toe om gebeurtenissen of *events* te detecteren en indien nodig de gepaste actie uit te voeren. Omdat gebeurtenissen zo vroeg in de operationele cyclus worden gecapteerd, kunnen ze uitval of verstoring vermijden. Event management is dus het proactieve proces dat aan incident beheer voorafgaat.

Beheer van gebeurtenissen is een preventieve maatregel.

2.1.2 Wat zijn gebeurtenissen?

Een gebeurtenis of *event* is een willekeurige meetbare of waarneembare verandering of voorkomen die betekenis heeft voor het beheren van de ICT-infrastructuur of voor het leveren van een ICT-dienst, en voor het evalueren van de impact die een afwijking op de dienst zou kunnen hebben.

Al wat materiële impact heeft op de zakelijke activiteiten komt in aanmerking, bvb:

- Omgevingsfactoren zoals wijziging in temperatuur, vochtigheidsgraad, vermogen;
- Intrusies;
- Foutenboodschappen;
- Boodschappen over het functioneren van een toepassing of systeem.

Het is voor een organisatie belangrijk om gebeurtenissen op te sporen en te analyseren en om passende actie te ondernemen. Voor het opsporen van gebeurtenissen moet de organisatie over geschikte methodes en monitoring beheerssystemen beschikken. Tevens moet die organisatie nauwkeurig hebben vastgelegd wanneer, uitgaande van een bepaalde basistoestand van haar infrastructuur, een waargenomen feit een gebeurtenis is volgens bovenstaande definitie.

2.1.3 Het verschil met incidenten

Wat is nu het verschil tussen een gebeurtenis of *event* en een incident?

Incidenten zijn ongeplande onderbrekingen of significante verminderingen in de kwaliteit van een ICT-dienstverlening. Zodra een incident zich voordoet, is er iets mis (voor meer informatie zie document: ‘Vo informatieclassificatie – Minimale maatregelen – incident beheer’)

Gebeurtenissen of *events* zijn wijzigingen in de status van de dienstverlening of configuratie-items.

Alle incidenten zijn dus gebeurtenissen, want een onderbreking of vermindering van de kwaliteit van een dienstverlening is een verandering in de status van die dienstverlening. Maar niet alle gebeurtenissen zijn incidenten, zoals bvb een verhoogd gebruik van een dienst (zolang binnen de eventueel gedefinieerde drempelwaarde), een gebruiker die inlogt, een geautomatiseerde back-up, …

2.1.4 Wat is beheer van gebeurtenissen?

Dit proces houdt zich bezig met de verwerking van gebeurtenissen aangegeven door het bron proces (het zakelijk proces, de toepassing, het systeem dat men wenst op te volgen), begrijpen wat ze betekenen en waar nodig de gepaste actie ondernemen, het is tevens de basis voor operationele monitoring en controle. Het proces beheer van gebeurtenissen registreert en interpreteert de wijziging

van de status van een systeem of dienst in een vroeg stadium, wat toelaat om in te grijpen vooraleer de gevolgen voor de zakelijke processen significant worden.

Elk systeem, proces of toepassing heeft de mogelijkheid om een triade aan gebeurtenissen te genereren. Het is dan ook niet mogelijk om alle gebeurtenissen te willen detecteren, opvolgen en beheren. Het is belangrijk om van meet af aan de juiste gebeurtenissen op te nemen in het beheersproces. Van bij het begin – de design fase van het bron proces – moet bekeken worden welke gebeurtenissen de moeite waard zijn om op te volgen.

Het begint dus met de identificatie van de gebeurtenissen die moeten worden opgevolgd: gaat het om reguliere operationele activiteit, is het ongewoon maar niet exceptioneel, of gaat het om een uitzondering? Deze gebeurtenissen moeten ontwikkeld en getest worden, de nodige tooling om deze gebeurtenissen te genereren, moet worden voorzien. Deze noodzakelijke eerste stap moet ondernomen worden in het bron proces en vormt de input van het proces beheer van gebeurtenissen.

Voor een veilige, stabiele en betrouwbare ICT-dienstverlening is het voor een ICT-organisatie belangrijk dat zij weet wat de 'normale' status is van haar ICT-infrastructuur en van haar ICT-diensten en dat zij vroegtijdig op de hoogte wordt gebracht van (dreigende) afwijkingen hiervan. Waargenomen gebeurtenissen kunnen een aanwijzing voor een dergelijke afwijking zijn. Ze worden meestal door een bewakings- of monitoringsysteem geregistreerd. Een gebeurtenis kan een normale situatie aangeven of een ongebruikelijke maar niet uitzonderlijke situatie, maar ook een ongebruikelijke handeling met potentieel gevaar. Afhankelijk van de zwaarte van de gebeurtenis moet (indien mogelijk geautomatiseerd) gepaste actie worden ondernomen.

Gebeurtenissen op het bron proces zijn een noodzakelijke input voor het proces beheer van gebeurtenissen; het bron proces moet dan ook volgende activiteiten voorzien (zie hoofdstuk: '*De bouwstenen van beheer van gebeurtenissen*')

- Detectie van gebeurtenissen;
- De typering vastleggen: informationele gebeurtenis, waarschuwing of uitzondering;
- Prioritering: toekennen van een prioriteit op basis van vooraf gedefinieerde regels (zoals bvb de criticiteit van het bron proces);
- Review activiteiten door het bronproces: werd er correct gereageerd.

Beheer van gebeurtenissen zelf omvat volgende activiteiten:

- Registratie van de gebeurtenis in het *event management* systeem;
- Filtering: bepalen of de gebeurtenis gecommuniceerd of genegeerd wordt (in dit laatste geval blijft enkel de log over);
- Correlatie: op basis van een vooraf gedefinieerde regels;
- Selectie van de response: enkel logging van de gebeurtenis, of automatische response, waarschuwing en menselijke tussenkomst.

2.1.5 Input voor het proces 'beheer van gebeurtenissen'

Zowat alle informatie die verwerkt wordt in het proces 'beheer van gebeurtenissen' is afkomstig uit systeem- en toepassingslogs. Bij de verwerking van die logs door het proces worden één of meer stappen uitgevoerd:

- **Collectie**: verzamelen van de loginformatie uit de systemen/toepassingen. Hierbij wordt een 'push' of 'pull' techniek gehanteerd. Bij 'pull' worden de logs op regelmatige tijdsstippen opgehaald waardoor het real-time gehalte daalt.

- **Normalisatie**: in deze stap wordt logs die verschillende formaten kunnen hebben (Windows Event log, Cysco log, syslog, …) omgezet naar een uniform formaat.
- **Correlatie**: hier worden verbanden gezocht tussen log informatie, ook al zijn deze op verschillende tijdsstippen en door verschillende systemen of toepassingen aangemaakt.
- **Verrijking**: sommige 'event management' systemen laten toe om extra informatie aan de logs te koppelen, bvb gekende kwetsbaarheden of de functie van een systeem/toepassing.

Logging kan elektronisch, maar ook manueel gebeuren (voor meer informatie zie document 'Vo Informatieclassificatie – Minimale maatregelen – SIEM'). Manuele waarnemingen van gebeurtenissen die erkend worden als een incident, worden verder elektronisch verwerkt in het incident beheerproces (voor meer informatie zie document 'Vo Informatieclassificatie - Minimale maatregelen – incident beheer').

2.1.6 Succesfactoren voor een goed beheer van gebeurtenissen

Een organisatie moet de kritische succesfactoren definiëren die passend zijn voor haar omgeving en elke kritische succesfactor moet opgevolgd worden door één of meerdere kritische prestatie-indicatoren (zie hoofdstuk: '*Meten is weten: prestatie-indicatoren (KPI's)*'). Succesfactoren voor beheer van gebeurtenissen omvatten:

- Identificatie van de statuswijzigingen die significant zijn voor een goed beheer van systemen, toepassingen en dienstverlening – het is cruciaal dat deze bij het bron proces correct worden gedefinieerd;
- Enkel een subset van gebeurtenissen vereist manuele interventie, maar het is wel belangrijk dat de juiste triggers gedefinieerd worden zodat – waar en wanneer nodig – deze interventie mogelijk is;
- Een correctie identificatie van 'normale situatie' en de middelen om te vergelijken ten opzichte van deze situatie.

2.1.7 *Event management* vs. monitoring

Hoe verschilt beheer van gebeurtenissen van monitoring? Beide processen zijn erg nauw verwant maar er zijn toch verschillen. Beheer van gebeurtenissen legt de focus op het verwerken van betekenisvolle meldingen over de status van de ICT-infrastructuur en dienstverlening. Monitoring is nodig om deze meldingen te detecteren en door te geven, maar monitoring werkt breder: monitoring zal bvb de status van een systeem controleren, ook als deze activiteit geen meldingen genereert. Beheer van gebeurtenissen verwerkt gebeurtenissen gegenereerd door monitoring, terwijl monitoring ook parameters bewaakt en opvolgt die geen gebeurtenissen genereren.

Het proces voor beheer van gebeurtenissen treedt enkel op wanneer een gebeurtenis zich voordoet, terwijl monitoring een continu proces is, dat werkzaam is zelfs als er geen gebeurtenis optreedt. Monitoring is dan ook een verlengde van beheer van gebeurtenissen.

2.2 De bouwstenen van beheer van gebeurtenissen

2.2.1 Detectie van een gebeurtenis

Gebeurtenissen komen 24x7 voor. Belangrijk voor een goed beheer van gebeurtenissen is de identificatie van die gebeurtenissen die significant zijn voor de dienstverlening en het opzetten van een systeem om deze te detecteren.

Detectie van gebeurtenissen vloeit voort uit systeem- en management tools. Vaak wordt SNMP als protocol hiervoor gebruikt, maar sommige gespecialiseerde management tools gebruiken een eigen, in-huis ontwikkeld protocol.

Een gebeurtenis is gelinkt aan een configuratie-item, deze configuratie-items zijn zodanig opgezet dat ze een vooraf gedefinieerde set gebeurtenissen genereren. Zoals eerder vermeld, gebeurt dit best in de design fase van het bron proces.

Zodra een gebeurtenis door het bron proces is aangemaakt, moet dit geregistreerd worden in het proces voor beheer van gebeurtenissen. De meeste configuratie-items communiceren gebeurtenissen op volgende wijze:

- Naar aanleiding van ondervraging door een beheerstool die bepaalde informatie van het systeem in kwestie opvraagt. Dit wordt *polling* genoemd.
- Het systeem kan ook gebeurtenissen genereren wanneer bepaalde vooraf ingestelde voorwaarden zijn vervuld.

Het is een goede praktijk om de gebeurtenissen altijd te loggen in het proces voor beheer van gebeurtenissen: een record van de gebeurtenis wordt aangemaakt samen met de bijhorende acties door het beheerssysteem of door de individuele toepassing, proces of hardware dat de gebeurtenis getriggerd heeft.

Triggers voor gebeurtenissen

Gebeurtenissen kunnen ontstaan vanuit eender welk type verandering of voorkomen. Het is zaak de juiste veranderingen of voorkomen te definiëren, d.w.z. die significant zijn en/of enige actie vereisen.

Voorbeelden van triggers zijn:

- Bepaalde waarden van performantie;
- Een uitzondering op een geautomatiseerde procedure of proces, bvb een routine is niet of niet tijdig uitgevoerd;
- Een uitzondering op een zakelijk proces dat gemonitord wordt;
- Vervolledigen van een geautomatiseerde taak of job;
- Een status wijziging van een systeem of record in een database;
- Toegang tot een toepassing of database door een gebruiker of een geautomatiseerde procedure of proces;
- Een situatie waarbij een gedefinieerde drempelwaarde is bereikt of overschreden.

Input voor het beheer van gebeurtenissen

Het bron proces levert meldingen van:

- Operationele en servicelevel vereisten;
- Alarmen, alerts en drempelwaarden voor het herkennen van gebeurtenissen;
- ‘Event correlatie’ tabellen, codes en geautomatiseerde antwoorden;
- Operationele procedures.

Daarnaast zijn er ook gebeurtenissen die de beschikbaarheid en integriteit van gebeurtenissen van het bron proces garandeert:

- Levert het bron proces nog steeds gebeurtenissen?
- Zijn deze gebeurtenissen betrouwbaar (= zijn ze inderdaad van het bron proces afkomstig)?

2.2.2 Typering van een gebeurtenis

Een gebeurtenis wordt ingedeeld in één van volgende categorieën:

- **Informationele gebeurtenis**: de gebeurtenis vereist geen onmiddellijke actie en is geen uitzondering. Ze worden bijgehouden in een logbestand gedurende een welbepaalde periode. Dit type gebeurtenis wordt gebruikt om de status van een systeem, toepassing of ICT-dienst te verifiëren of om statistische informatie te verzamelen, of om beter inzicht te verwerven voor besluitvorming.
- **Waarschuwing** (*warning*/alert): deze gebeurtenis wordt gegenereerd zodra een systeem, toepassing of ICT-dienst een vooraf bepaalde drempelwaarde nadert (*threshold*). Waarschuwingen worden gebruikt om de aandacht te vestigen op een potentieel naderend probleem zodat er kan worden ingegrepen vooraleer een uitzondering optreedt.
- **Uitzondering** (*exception*/error): dit houdt een gedegradeerde ICT-dienstverlening in, wat wil zeggen dat een systeem, toepassing of ICT-dienst onder het niveau van de normale parameters of indicatoren functioneert. Er zijn gevolgen voor de zakelijke processen, bvb door een verminderde performantie, verlies van functionaliteit of uitval van een ICT-dienst of systeem/toepassing.

2.2.3 Filteren van gebeurtenissen

Dit houdt in dat een gebeurtenis kan worden gecommuniceerd of genegeerd. Indien de gebeurtenis genegeerd wordt, moet zij in ieder geval gelogd worden, maar er wordt geen verdere actie aan gegeven.

Filtering is een essentieel onderdeel van beheer van gebeurtenissen om redundante en onnodige informatie te vermijden.

Filtering is nodig:

- De hoeveelheid informatie gegenereerd door de systemen, toepassingen en ICT-diensten mag niet onderschat worden. Alle informatie over gebeurtenissen ongefilterd doorlaten zou het proces overbelasten.
- Vaak wordt dezelfde informatie onder vorm van verschillende gebeurtenissen gegenereerd. Deze redundante gebeurtenissen herkennen en herleiden tot één stuk informatie kan de efficiëntie en beheersbaarheid alleen maar verhogen.
- De impact op bandbreedte en netwerk capaciteit kan door filtering onder controle gehouden worden.

2.2.4 Correlatie van gebeurtenissen

Correlatie wordt meestal uitgevoerd door een *correlation engine* die vaak deel uitmaakt van een *event management* tool. Correlatie houdt in dat gebeurtenissen worden vergeleken volgens een vooraf gedefinieerde reeks criteria en regels in een bepaalde volgorde, ook *business rules* genoemd. Aan de hand van correlatie wordt de impact van de gebeurtenis op de zakelijke processen ingeschat.

Voorbeelden van correlatie zijn:

- Aantal gelijkaardige gebeurtenissen (bvb verschillende inlogpogingen van een gebruiker);
- Aantal configuratie-items die dezelfde gebeurtenis genereren;
- Nagaan of een bepaalde actie is gekoppeld aan de code of data waarover de gebeurtenis bericht;
- Of het om een uitzondering gaat;
- Vergelijking met een minimum of maximumwaarde (is een bepaalde grens overschreden?);

- Of bijkomende informatie nodig zijn om de gebeurtenis verder te analyseren, eventueel door het ophalen van informatie uit een ander systeem.

Aan de hand van vooraf gedefinieerde regels kan de *correlation engine* ook een prioriteit toekennen aan de gebeurtenis.

2.2.5 Reactie op een gebeurtenis

Er zijn verschillende mogelijkheden om te reageren op gebeurtenissen, in algemene termen kan gesteld worden:

- **Automatische response:** hierbij wordt een actie getriggerd op de gebeurtenis zonder menselijke tussenkomst.
- **Menselijke interactie**: deze gebeurtenissen moeten worden geëscaleerd naar de juiste personen zodat actie kan worden ondernomen.
- **Aanmaken van een incident** record: een gebeurtenis van categorie uitzondering moet verder opgenomen worden in het proces incident beheer. Ook een waarschuwing kan verder afgehandeld worden in het proces incident beheer.

2.2.6 Review van een actie

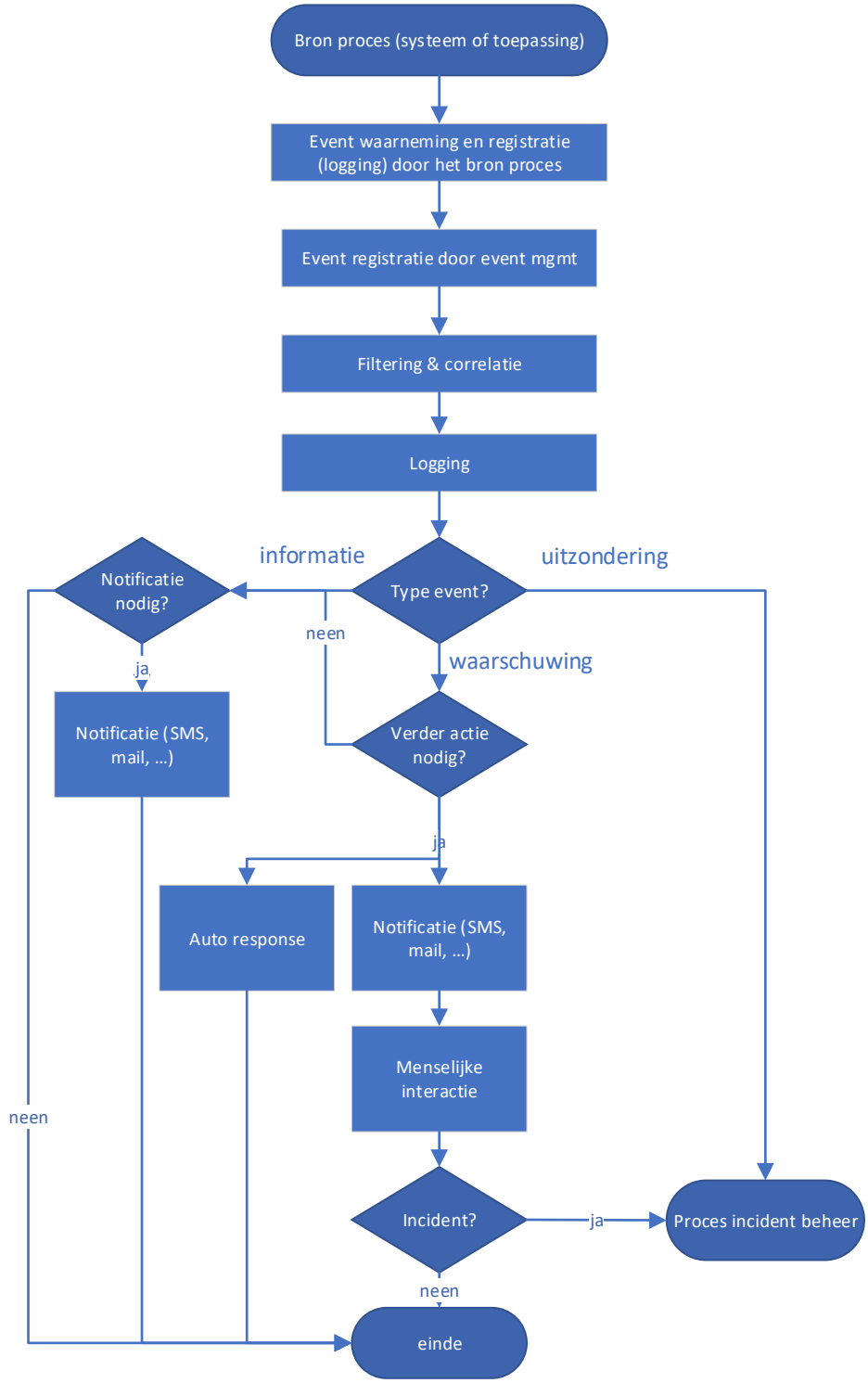
Ingeval een gebeurtenis aanleiding geeft tot een interactie, dan zou het resultaat ervan best geverifieerd worden door het bron proces. Dit kan eventueel automatisch gebeuren, bvb door het uitvoeren van een script om te kijken of het systeem of de toepassing correct werkt.

Waar de gebeurtenis aanleiding geeft tot een incident of wijziging houdt de review een verificatie van de juiste overdracht naar het incident- of wijzigingsproces in.

Gebeurtenissen worden niet altijd afgesloten:

- Gebeurtenissen die een incident of wijziging genereren, moeten formeel afgesloten worden. Afsluiten van een gebeurtenis moet steeds gevolgd worden door een review van de genomen acties.
- Gebeurtenissen van het type ‘informationele gebeurtenis’ worden gelogd en eventueel als input voor andere processen gebruikt en hoeven niet formeel afgesloten te worden.

2.2.7 Het proces



3. LINK MET ANDERE BEHEERPROCESSEN

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

Primair heeft het interactie met:

- Incident beheer:
  (Zie document: 'Vo Informatieclassificatie - Minimale maatregelen - incident beheer')
- Wijzigingsbeheer:
  (Zie document: 'Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer')
- Log beheer:
  (Zie document: 'Vo Informatieclassificatie - Minimale maatregelen – SIEM')
- Monitoring:
  (Zie document: 'Vo Informatieclassificatie - Minimale maatregelen – SIEM')

Maar er is ook een link met:

- Capaciteitsbeheer voor een beter begrip en fine-tuning van de geïdentificeerde gebeurtenissen, drempelwaarden enz.;
- Beheer van middelen voor het beheer van de status van *assets* of bedrijfsmiddelen;
- Asset en configuratie beheer voor het beheer van de status van configuratie-items.9
  (Zie document: 'Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer'*)*

4. PRESTATIE-INDICATOREN (KPI'S)

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

- Aantal gebeurtenissen vergeleken met aantal incidenten;
- Aantal en percentage gebeurtenissen per type gebeurtenis en per systeem, toepassing of dienst ten opzichte van het totaal aantal systemen, toepassingen of diensten;
- Aantal gebeurtenissen waar manuele interventie nodig was;
- Aantal gebeurtenissen dat geleid heeft tot een incident t.o.v. totaal aantal gebeurtenissen;
- Aantal gebeurtenissen dat geleid heeft tot een wijziging t.o.v. totaal aantal gebeurtenissen.

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 proces.