Informatieclassificatie Vlaamse overheid (Vo-ICR)

Veiligheidslogging en monitoring (SIEM)

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 SIEM. 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 3 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.

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	16 maart 2018	Kristel VAN AKEN	Eerste draft
v.0.2		Kristel VAN AKEN	Feedback Johan Smekens verwerkt
v.0.3	10 april 2018	Kristel VAN AKEN	Monitoring, SIEM en vereisten KSZ toegevoegd
v.0.4	26 april	Johan SMEKENS	Review
v.0.5	30 april 2018	Kristel Van Aken	Feedback Johan Smekens verwerkt
v.1.0	2 mei 2018	Johan SMEKENS	Publicatie
v.1.1	11 september 2018	Kristel Van Aken	Link met andere maatregelen bijgewerkt
v.1.2	18 december 2019	Kristel VAN AKEN	Feedback leespanel en consistentie check
v.1.3	06 augustus 2020	Kristel VAN AKEN	Integriteit toevoegen
v.1.4	10 augustus 2020	Johan SMEKENS	Review/Opmerkingen
v.1.5	28 september 2020	Kristel VAN AKEN	Feedback werkgroep informatieveiligheid
v.1.6	10 juni 2021	Kristel VAN AKEN	Beschikbaarheid toevoegen
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 – Cryptografie*
  - *Vo Informatieclassificatie - Minimale maatregelen – PAM*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)
- https://www.noraonline.nl/wiki/NORA_online

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

Inhoudsopgave

INLEIDING

Audit logs bestaan uit systeem informatie gebruikt om systeem- en gebruikersactiviteiten op te sporen en te koppelen aan gebeurtenissen (*events*). Gebruik makend van de juiste tools en procedures kunnen audit logs bijdragen tot de detectie van inbreuken op informatie- en ICT-veiligheid, het opsporen van technische problemen en non-conformiteit t.o.v. beleidslijnen.

Monitoring gaat nog een stap verder door (*near*) real-time opvolging van gebeurtenissen.

Logging bestaat uit het verzamelen en bijhouden van informatie; deze informatie wordt op haar beurt gebruikt voor relevante opvolging en dient als controle input voor de beveiliging en risicobeheersing.

In oplopende volgorde van complexiteit bestaat het loggen uit:

- Manuele logboeken,
- Geautomatiseerde audit logs,
- Audit trails.

Er worden verschillende geautomatiseerde audit logs erkend:

- Technische logs of systeem logs: hierin worden gebeurtenissen (events) opgenomen zoals het gebruik technische en functionele beheersfuncties, activiteiten onder beveiligingsbeheer, verstoringen en (veiligheids-)incidenten. Voorbeelden van veiligheidsincidenten zijn: detectie van malware, foutieve inlogpogingen (hiervoor wordt een drempelwaarde bepaald), overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices en het starten en stoppen van security services. Voorbeelden van verstoringen in het productieproces zijn: vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur en het niet beschikbaar zijn van aangeroepen programmaonderdelen of –systemen.
- Applicatie logs: verzamelt gebeurtenissen van een toepassing zoals berichten, uitzonderingen en fouten. Het formaat en de inhoud van deze logs wordt bepaald tijdens de design fase van een toepassing. Applicatie logs worden ook wel functionele logs genoemd, een bijzondere vorm hiervan is transactionele logging, waarbij informatie uit transacties worden bijgehouden.

Het verwerken van de log informatie, ook weer in oplopende volgorde van complexiteit, bestaat uit:

- Analyse van de audit logs, bij voorkeur a.d.h.v. filtering tools,
- Correlatie van diverse audit logs, al dan niet met externe bronnen,
- (Real-time) veiligheidsmonitoring,
- Security incident & event monitoring (SIEM).

Merk op dat de complexiteit gepaard gaande met automatisatie omgekeerd evenredig is met de operationele middelen (mankracht – tijd) nodig om de taak uit te voeren.

Manuele logging is het handmatig bijhouden van activiteiten en registratie ervan in een logboek. Het spreekt voor zich dat deze methode het meest gevoelig is voor fouten, onregelmatigheden en het ontbreken van activiteiten, daar deze gebaseerd is op de discipline en de capaciteit van de uitvoerders om deze taak systematisch en precies te herhalen. Bovendien zijn er vaak meerdere uitvoerders bij betrokken, wat eenzelfde methodiek en discipline noodzaakt. Een voorbeeld waar manuele logging wel vaak gebruikt wordt, is het bezoekerslogboek.

De eerste stap bij het opzetten van een succesvol audit programma, is het identificeren en documenteren van de te loggen activiteiten, en hun onderlinge relaties, die relevantie hebben met het beoogde doel. Hierbij worden volgende types onderscheiden:

〉 Gebruikersactiviteiten: dit is elke menselijke tussenkomst in een proces (creatie, consultatie, wijziging, verwijdering). Deze tussenkomst omvat ook het gebruik van geprivilegieerde accounts;

Systeemactiviteiten: bvb systeemfouten, *shutdown*/*restart*, enz.

Een volgende stap is het opzetten van een goede audit infrastructuur, deze ziet er globaal genomen zo uit:

〉 Log informatie genereren d.m.v. parametrisatie van lokale systemen,

Parametrisatie van lokale systemen zodat zij audit records (*events*) verzamelen,

Deze informatie wordt vanuit de lokale systemen in een log beheer platform verzameld. Dit kan een bestand of een database zijn die lokaal of centraal opgeslagen wordt. Het log beheer platform bewaakt de integriteit en beheert de *lifecycle* van de verzamelde log informatie (*events*),

〉 Een log analyse tool maakt gebruik van deze centrale database aan audit records,

〉 Er is tevens back-up van logbestanden voorzien,

〉 Bijhouden op lange termijn via een archivage systeem.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Log informatie krijgt minimaal informatieklasse 2 voor vertrouwelijkheid toegewezen. 〉 Gebruik van geprivilegieerde accounts (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – PAM*') 〉 Applicatie logs: cryptografische maatregelen i.v.m. log informatie zijn op hetzelfde niveau als de toepassing waaruit de log info aangemaakt wordt: zie document 'Vo Informatieclassificatie - Minimale maatregelen – Cryptografie' 〉 Logging/auditing van gebeurtenissen i.h.k.v. vertrouwelijkheid: 〉 Log policy opzetten voor alle systemen en toepassingen, 〉 Logging opzetten ter ondersteuning van het event en incidentproces: 〉 Type gebeurtenis, 〉 Waar en wanneer de gebeurtenis plaats vond, 〉 Oorzaak en gevolg van de gebeurtenis, 〉 Accounts gelinkt aan de gebeurtenis. 〉 Monitoring van verwijderen van loginformatie (*clear log events*) 〉 Beschermen van audit records: vertrouwelijkheid garanderen d.m.v. fysieke beveiliging en logische toegangscontrole.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Log informatie krijgt minimaal informatieklasse 3 voor vertrouwelijkheid toegewezen. 〉 Beschermen van audit records: vertrouwelijkheid garanderen d.m.v. cryptografische maatregelen: zie document '*Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*' 〉 Logging/auditing van gebeurtenissen i.h.k.v. vertrouwelijkheid: 〉 Audit trail voor gebruik van systeemhulpmiddelen. 〉 Audit trail voor verwerking van informatie. 〉 Periodieke analyse van audit records. 〉 Gebruik maken van tools voor analyse en rapportering 〉 Jaarlijks de auditfunctie evalueren.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 +

	〉 Log informatie krijgt minimaal informatieklasse 4 voor vertrouwelijkheid toegewezen. 〉 Logging/auditing van gebeurtenissen i.h.k.v. vertrouwelijkheid: 〉 Logging integreren met scanning en monitoring capaciteiten. 〉 Event correlatie toepassen. 〉 Centraal beheer van logbestanden 〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie. 〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit.

Integriteit

IC klasse	Minimale maatregelen

	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	〉 Log informatie krijgt minimaal informatieklasse 2 voor integriteit toegewezen.
	〉 Applicatie logs: cryptografische maatregelen i.v.m. log informatie zijn op hetzelfde niveau als de toepassing waaruit de log info aangemaakt wordt: zie document '*Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*'
	〉 Logging/auditing van gebeurtenissen i.h.k.v. integriteit:
	  〉 Log policy opzetten voor alle systemen en toepassingen,
	〉 Logging opzetten ter ondersteuning van het event en incidentproces:
	  〉 Type gebeurtenis,
	  〉 Waar en wanneer de gebeurtenis plaatsvond,
	  〉 Oorzaak en gevolg van de gebeurtenis,
	  〉 Accounts gelinkt aan de gebeurtenis.
	〉 Monitoring van *clear log* gebeurtenissen
	〉 Beschermen van audit records: integriteit garanderen d.m.v. fysieke beveiliging en logische toegangscontrole.
	〉 *Timestamps* op audit records: kloksynchronisatie toepassen.
	〉 Toegang tot audit records beperken tot consultatie functie (*read only*)

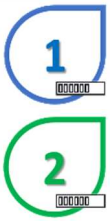
	Alle maatregelen van Klasse 1 / Klasse 2 +
	〉 Log informatie krijgt minimaal informatieklasse 3 voor integriteit toegewezen.
	〉 Beschermen van audit records: integriteit garanderen d.m.v. cryptografische maatregelen: zie document '*Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*'
	〉 Logging/auditing van gebeurtenissen i.h.k.v. integriteit:
	  〉 Audit trail voor gebruik van systeemhulpmiddelen.
	  〉 Audit trail voor verwerking van informatie.
	  〉 *Timestamps*: kloksynchronisatie met goedgekeurde externe tijdsbron.
	  〉 Periodieke analyse van audit records.
	  〉 Gebruik maken van tools voor analyse en rapportering

	〉 Jaarlijks de auditfunctie evalueren.

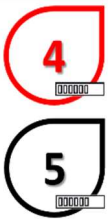
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen:
	
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 +
	
	〉 Log informatie krijgt minimaal informatieklasse 4 voor integriteit toegewezen.
	〉 Logging/auditing i.h.k.v. integriteit:
	  〉 Logging integreren met scanning en monitoring capaciteiten.
	  〉 *Timestamps* in combinatie met digitale handtekening toepassen.
	  〉 Event correlatie toepassen.
	〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie.
	〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit.

Beschikbaarheid

IC klasse	Minimale maatregelen

	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	
	〉 Log informatie krijgt minimaal informatieklasse 2 voor beschikbaarheid (omwille van kritisch bedrijfsmoment, bvb na een incident en herstel van log informatie) toegewezen.
	〉 Logging/auditing van gebeurtenissen i.h.k.v. beschikbaarheid:
	  〉 Log policy opzetten voor alle systemen en toepassingen,
	〉 Logging opzetten ter ondersteuning van het event en incidentproces:
	  〉 Type gebeurtenis,
	  〉 Waar en wanneer de gebeurtenis plaatsvond,
	  〉 Oorzaak en gevolg van de gebeurtenis,
	  〉 Accounts gelinkt aan de gebeurtenis.
	〉 Monitoring van verwijderen van loginformatie (*clear log events*)
	〉 Retentie: log informatie lokaal bewaren.
	〉 Backup: log informatie opnemen in het backupschema.
	〉 Beschermen van audit records: beschikbaarheid garanderen d.m.v. fysieke beveiliging en logische toegangscontrole.

	Alle maatregelen van Klasse 1 / Klasse 2 +
	
	〉 Log informatie krijgt minimaal informatieklasse 3 (omwille van kritisch bedrijfsmoment, bvb na een incident en herstel van log informatie) voor beschikbaarheid toegewezen.
	〉 Logging/auditing van gebeurtenissen i.h.k.v. beschikbaarheid:
	  〉 Audit trail voor gebruik van systeemhulpmiddelen.
	  〉 Audit trail voor verwerking van informatie.

	〉 Periodieke analyse van audit records. 〉 Gebruik maken van tools voor analyse en rapportering 〉 Centrale opslag van loginformatie. 〉 Retentieperiode van lokale loginformatie beperken tot *caching* (tot centrale opslag geverifieerd gelukt is). 〉 Backup: 〉 Backups regelmatig verifiëren op succesvolle aanmaak; 〉 Periodiek testen op herstelprocedures (*recovery*). 〉 Jaarlijks de auditfunctie evalueren. 〉 Alarmen genereren en opvolgen als opslagcapaciteit voor logbestanden 80% bereikt heeft. 〉 Fysieke beveiliging: reserveonderdelen of redundant uitvoeren van omgeving. 〉 Retentie: lange termijn bewaring/archivering van log informatie conform wet- en regelgeving.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Log informatie krijgt minimaal informatieklasse 4 (omwille van kritisch bedrijfsmoment, bvb na een incident en herstel van log informatie) voor beschikbaarheid toegewezen. 〉 Logging/auditing van gebeurtenissen i.h.k.v. beschikbaarheid: 〉 Logging integreren met scanning en monitoring capaciteiten. 〉 Event correlatie toepassen. 〉 Centraal beheer van logbestanden 〉 Backup: rapportering over backup/recovery testen aan toepassingseigenaar, CISO/DPO 〉 Fysieke beveiliging: redundantie inregelen en periodiek testen met rapportering aan toepassingseigenaar, CISO/DPO. 〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie. 〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit.

1.2 Minimale specifieke (GDPR) maatregelen

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

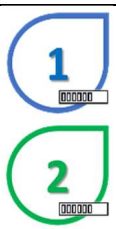
Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1 en Klasse 2.
	Klasse 3 maatregelen: 〉 Event correlatie toepassen. 〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie. 〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit. 〉 Elke toegang tot persoonsgegevens, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving: 〉 Tot natuurlijke persoon herleidbare gebruikersnaam of ID, tijdsstip (datum/uur), identificatie van het werkstation of locatie, gebruikte toepassing. 〉 De persoon die het object is van de handeling 〉 Het resultaat van de handeling
	Klasse 4 maatregelen: Alle maatregelen van Klasse 3 + 〉 Elke toegang tot gegevens behorende tot de bijzondere categorieën van de GDPR, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving.
	Er zijn geen GDPR specifieke maatregelen voor Klasse 5.

Integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1 en Klasse 2.
	Klasse 3 maatregelen: 〉 *Timestamps* in combinatie met digitale handtekening toepassen. 〉 Event correlatie toepassen. 〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie. 〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit. 〉 Elke toegang tot persoonsgegevens, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving: 〉 Tot natuurlijke persoon herleidbare gebruikersnaam of ID, tijdsstip (datum/uur), identificatie van het werkstation of locatie 〉 De persoon die het object is van de handeling 〉 Het resultaat van de handeling
	Klasse 4 maatregelen: Alle maatregelen van Klasse 3 + 〉 Elke toegang tot persoonsgegevens behorende tot de bijzondere categorieën van de GDPR moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving.
	Er zijn geen GDPR specifieke maatregelen voor Klasse 5.

Beschikbaarheid

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1 en Klasse 2.

	Klasse 3 maatregelen:
	
	〉 Event correlatie toepassen.
	〉 Real-time alarmen genereren en opvolgen bij problemen met de auditfunctie.
	〉 4-ogen toepassen bij elke wijziging aan de audit functionaliteit.
	〉 Elke toegang tot persoonsgegevens, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving:
	  〉 Tot natuurlijke persoon herleidbare gebruikersnaam of ID, tijdsstip (datum/uur), identificatie van het werkstation of locatie, gebruikte toepassing.
	  〉 De persoon die het object is van de handeling
	  〉 Het resultaat van de handeling

	Klasse 4 maatregelen: Alle maatregelen van Klasse 3 + 〉 Elke toegang tot gegevens behorende tot de bijzondere categorieën van de GDPR, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving.
	Er zijn geen GDPR specifieke maatregelen voor Klasse 5.

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

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

Beschikbaarheid, Vertrouwelijkheid en Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Elke organisatie moet: ○ Een formele procedure van logbeheer opzetten, valideren, communiceren en onderhouden. ○ Transacties, controlewerkzaamheden, activiteiten van gebruikers, uitzonderingen en informatieveiligheid- en privacy-gebeurtenissen/incidenten gestructureerd vastleggen in afzonderlijke logbestanden, zodat iedere handeling naar de brondocumenten herleid kan worden of de uitgevoerde bewerking(en) gecontroleerd kan(kunnen) worden. ○ Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren. ○ Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving. ○ De interne klokken van alle informatiesystemen van de organisatie moeten gesynchroniseerd worden met een overeengekomen nauwkeurige tijdsbron zodat een betrouwbare analyse van logbestanden op verschillende informatiesystemen altijd mogelijk is. ○ De noodzakelijke tools moeten beschikbaar zijn of ontwikkeld worden om log gegevens te kunnen laten analyseren door de geautoriseerde personen. ○ Systeemgebruik moet zoveel als mogelijk automatisch worden gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een manueel logboek door systeembeheerders. ○ Logbestanden moeten beschermd worden tegen inzage door onbevoegden, wijzigingen en verwijderingen. ○ De logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving. ○ De raadpleging van logbestanden moet altijd het voorwerp zijn van een georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd. ○ Het resultaat van logbeheer moet regelmatig geanalyseerd, gerapporteerd en beoordeeld worden (Ref. KSZ 5.9.5).

	〉 Elke organisatie moet: o Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, loggen in overeenstemming met de beleidslijnen “logging” en de toepasselijke wetgeving en regelgeving (Ref. KSZ 5.11.7 a). o In de specificaties van een project opnemen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen van de beleidslijnen informatieveiligheid en privacy. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen: ▪ a. Glashelder, snel en eenvoudig kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie ▪ b. De identificatie van de aard van de geraadpleegde informatie ▪ c. De duidelijke identificatie van de persoon (Ref. KSZ 5.11.7 b). o Rekening houden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project (Ref. KSZ 5.11.7 c). o De noodzakelijke tools ter beschikking hebben of ontwikkelen om toe te laten deze log gegevens uit te baten door de geautoriseerde personen (Ref. KSZ 5.11.7 d). o De algemene regel toepassen dat de transactionele/functionele log gegevens minimaal 10 jaar en de technische/infrastructurele log gegevens minimaal 2 jaar moeten bewaard blijven (Ref. KSZ 5.11.7 e).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Logging als maatregelen

2.1.1. Kenmerken van de logging maatregelen

Een audit log is een verzameling chronologische records (een flat file, gestructureerd bestand, database of fysiek logboek) deze verzameling voert bewijs aan van een activiteit of geheel van activiteiten in een verwerking, procedure of gebeurtenis.

Een audit trail is een beveiligde en geautomatiseerde verzameling chronologische records, deze verzameling (een flat file, gestructureerd bestand, database of fysiek logboek), laat toe om een reeks gebeurtenissen te reconstrueren volgens hun tijdsstip van voorkomen en gerelateerd aan de aanmaak, wijziging en verwijdering van elektronische records. Dankzij deze structuur is de audit informatie toegankelijker en makkelijker te ontginnen dankzij het gebruik van analyse tools.

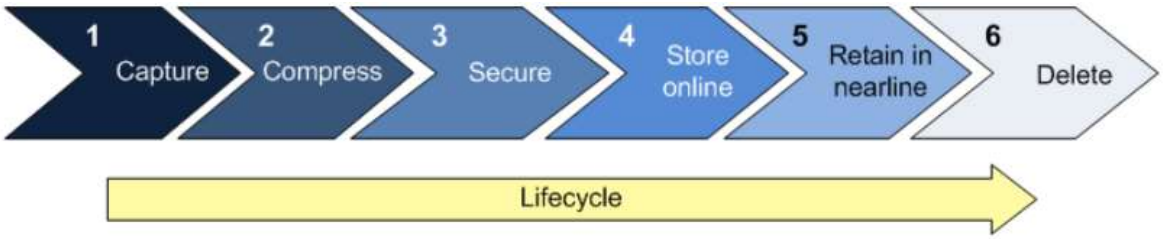
Als dusdanig zijn audit logs en trails een belangrijke beveiligingsmaatregel:

- Preventief: door opvolgen van informatie uit audit logs is het mogelijk om bvb de eerste signalen van een cyberaanval te herkennen, waarna stappen kunnen worden ondernomen om deze aanval te stoppen en/of verdere gevolgen te voorkomen;
- Reactief: door log analyse en correlatie met andere informatiebronnen achterhalen wat er precies is gebeurd:
- Ter ondersteuning van het proces risico beheer
- Ter ondersteuning van het proces probleembeheer;
- Lering trekken uit incidenten;
- Bewijsvoering – juridische bewijsvoering;
- Voor statistisch gebruik.

Audit log beheer omvat een aantal processen:

- Identificatie van de systemen waarop audit logging moet worden geactiveerd (werkstations, servers, databases, middleware, speciale apparatuur zoals firewalls, proxy, routers, enz.),
- Configuratie van het log beheer op de relevante configuraties,
- Creatie van audit logs,

Lifecycle beheer van de log informatie: de *lifecycle* van log informatie omvat volgende fasen: aanmaak, formattering, beveiliging, online opslag, archivering (off-line retentie) en vernietiging,



- Opslaan, archivering en verwijderen van audit logs,
- Review en analyse van audit log resultaten, rapportering.

De nodige procedures moeten opgezet worden om intern onderzoek, forensische analyse, vastleggen van technische baselines en identificatie van lange-termijn trends te ondersteunen.

Bronnen voor logging

Er zijn vele verschillende soorten mechanismen voor logging van componenten die naast elkaar kunnen voorkomen. Voorbeelden van deze mechanismen zijn:

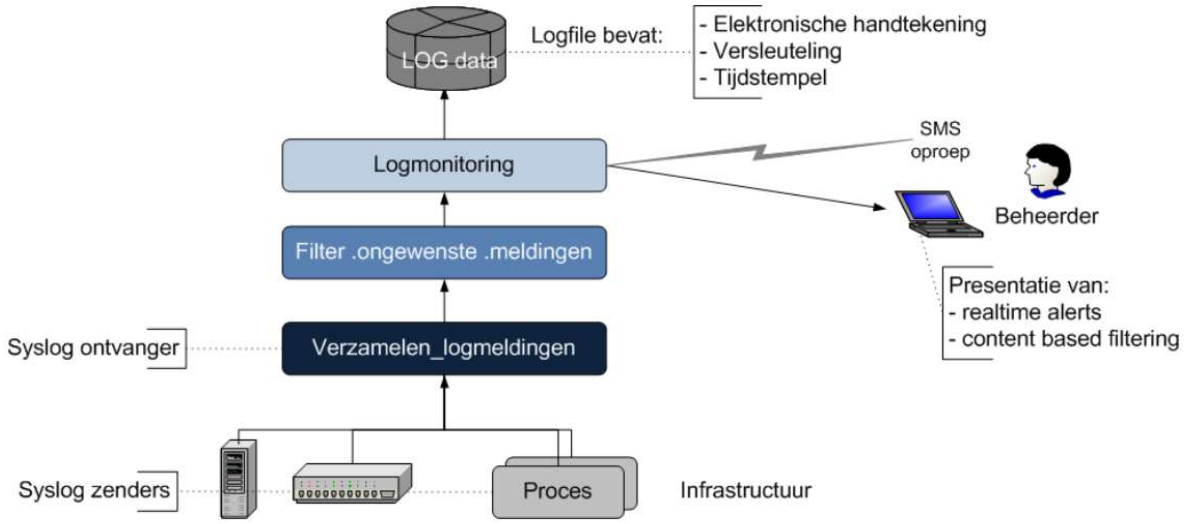
- SYSLOG is een standaard voor computerlogging. De logging is gescheiden tussen systemen die de logging genereren en systemen die de logging opslaan.

SNMP staat voor *Simple Network Management Protocol*. Dit protocol kan worden gebruikt voor het besturen van netwerkapparaten. Het protocol voorziet ook in statusmeldingen (*traps*).
De *Windows Event log* is standaard in de Windows-besturingssystemen aanwezig en kan ook naar een centrale logvoorziening worden verzonden.

- Losse logbestanden zoals tekstbestanden, komma gescheiden (CSV) bestanden en andere varianten.
- Vanuit applicaties en binnen databases wordt vaak gelogd binnen de database zelf of een aparte database. Deze logging is doorgaans gestructureerd en ook door te zenden aan een centraal logsysteem.

Logging van beveiligingssystemen, zoals *Intrusion Detection Systems*

Een systeem voor logging zou er dan bijvoorbeeld zo kunnen uitzien:



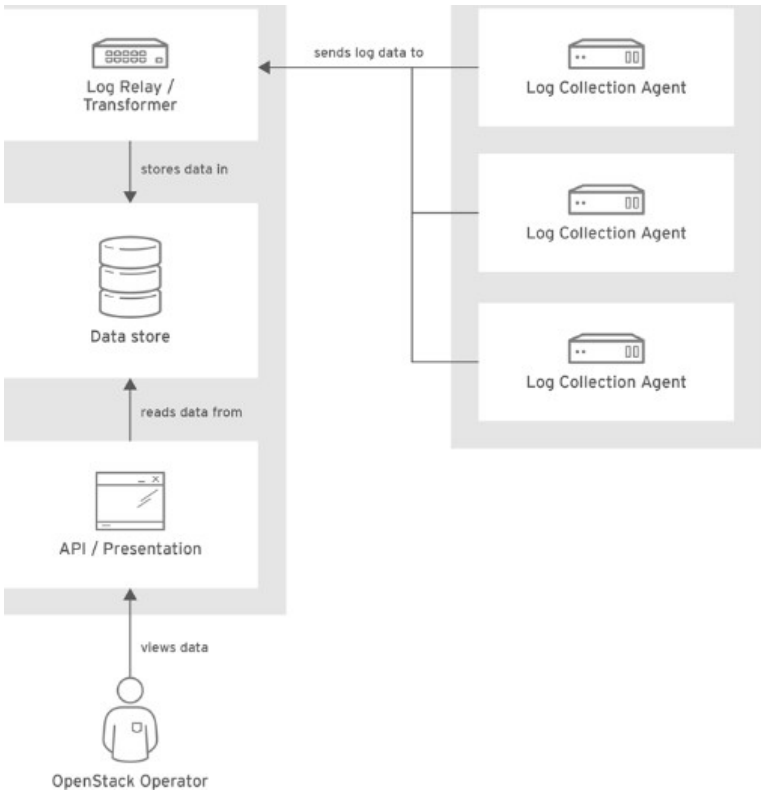
Lokale versus centrale opslag

Door de verschillende mechanismen voor logging loopt een organisatie het risico om het overzicht over alle gebeurtenissen kwijt kan raken. Om bijvoorbeeld aanvallen efficiënt te kunnen detecteren is het belangrijk de log informatie op één centraal punt op te slaan, waardoor een duidelijk zicht op alle informatie vanuit de verschillende componenten uit de infrastructuur mogelijk is. Het voordeel van centraal loggen is:

- Gebruiksgemak: Er hoeft maar op één plaats gekeken te worden.
- Beschikbaarheid: De logging is beschikbaar, ook als het systeem dat logt niet beschikbaar is.
- Veiligheid: De logging is ook beschikbaar als het bronsysteem gehackt of besmet is.
- Veiligheid: De logging kan worden afgeschermd tegen onbevoegd inzien en modificatie, bijvoorbeeld door digitaal ondertekenen.
- Eenvoud: Een centrale logging is eenvoudiger veilig te stellen op bijvoorbeeld een back-up.
- Automatische analyse van logbestanden geeft sneller de samenhang van incidenten weer en maakt het mogelijk om logische verbanden tussen geïsoleerde incidenten te detecteren, zoals een systeeminbraak die zich in meerdere, verschillende stappen laat herkennen.

Toch ontkomt men niet aan het lokaal bijhouden van log informatie: dit is immers nodig om de coherentie en consistentie van de log informatie te garanderen: de log informatie moet minstens zolang lokaal worden bijgehouden tot er een bevestiging van goed ontvangst van de log informatie door het centrale opslagsysteem.

Een centraal opgezette logging architectuur ziet er schematisch als volgt uit[1]:



Auditeerbare gebeurtenissen

Hiermee worden de geïdentificeerde activiteiten voor logging bedoeld:

- Succes en falen van aanloggen,
- Succes en falen van authenticatie,
- Succes en falen in autorisatie,
- Succes en falen in het uitvoeren van geprivilegieerde activiteiten,
- Succes en falen in toegang tot bestanden, folders, toepassingen en systeemtools,
- Succes en falen in toegang tot functionele en technische beheersfuncties,
- Creatie, wijziging, verwijdering van accounts, bestanden, folders,
- Creatie, wijziging, verwijdering van systeem parameters (inclusief database),

Creatie, wijziging, verwijdering in *policies*,

- Creatie, wijziging, verwijdering in toegangsparameters zoals rechten en privileges,

Creatie - en toepassingsactiviteiten zoals *shutdown*, reboot, fouten,

- Wijzigingen aan systemen en toepassingen.

Daarnaast moet men ook de nodige drempelwaarden (*thresholds*) zetten: vanaf welke grens wordt een auditeerbare gebeurtenis aanzien als een (potentieel) incident.

Inhoud van audit records

Audit records moeten voldoende informatie bevatten om – eventueel in aggregatie met andere informatiebronnen – weer te geven welke gebeurtenis heeft plaats gevonden, wat de oorzaak en wat de gevolgen zijn. Daarnaast moet het mogelijk zijn om elke menselijke interventie in verband met een gebeurtenis te identificeren.

Een correct geïmplementeerde log moet antwoord kunnen bieden op volgende vragen:

- Wat gebeurde er?
- Wanneer gebeurde het?
- Waar gebeurde het?
- Wie was betrokken?
- Waar komt het vandaan?

Concreet betekent dit voor het opzetten van een succesvolle audit trail:

- Datum en tijdsstip,
- Userid/domein, herleidbaar tot een persoon, systeem, locatie,
- Bron IP of toepassing,
- Gebruikte toepassing, URL of service,
- Gebruikte module of functie,
- Uitgevoerde actie (creatie, wijziging, consultatie, verwijdering),
- Dataveld gewijzigd of geconsulteerd.

Retentie en beveiliging van audit records

Audit records moeten op een beveiligde manier opgeslagen worden en bijgehouden om analyse toe te laten. Dit houdt in:

Er moet een *lifecycle* model op de log data toegepast worden rekening houdend met de operationele beschikbaarheid en de archivering van log data.

- Enkel geautoriseerde personen mogen toegang hebben tot de audit records en log bestanden.
- Audit records mogen niet gewijzigd, overschreven of verwijderd worden.
- Paramaters van het audit systeem mogen enkel gewijzigd worden door geautoriseerd personeel en met toepassing van het 4-ogen principe.
- Audit records moeten beschikbaar zijn voor analyse en rapportering wanneer nodig, bvb in geval van een intern of extern onderzoek. Bovendien moeten ze voldoende lang worden bijgehouden, in lijn met de toepasbare wet- en regelgeving. Dit betekent ook dat voldoende opslagcapaciteit – eventueel offline – beschikbaar moet zijn en dat er rekening moet worden gehouden met potentiële impact op performantie van het systeem/de toepassing.

Audit records kunnen informatie bevatten van een bepaalde informatieklasse. Deze records en de logbestanden zelf moeten dan ook minstens dezelfde informatieklasse krijgen. Zo zal bvb een security log op toepassingen met persoonsgegevens minstens dezelfde klasse krijgen als de persoonsgegevens zelf.

Beveiliging van logbestanden

Ook logbestanden moeten beveiligd worden tegen niet-geautoriseerde toegang. De log zelf moet dezelfde informatieklasse toegewezen krijgen als de informatieklasse van de informatie die ze beschermt, indien deze informatie opgenomen is in de logs en bijgevolg moeten de bijhorende maatregelen ook op de log informatie toegepast worden. Dit geldt dus vooral voor applicatie logs en in mindere mate voor systeem logs, omdat deze laatste meestal geen applicatieve informatie bevatten. Volgende maatregelen moeten toegepast worden om de vertrouwelijkheid, integriteit en beschikbaarheid van log informatie te garanderen doorheen de volledig levenscyclus van de log informatie:

- Vertrouwelijkheid:
  - Fysieke of logische toegangscontrole;
  - Versleuteling van de log informatie.
- Integriteit:
  - *Read only* toegang tot log informatie verzekeren;
  - Functiescheiding toepassen;
  - Log informatie centraal opslaan;
  - Time stamping en digitaal tekenen.
- Beschikbaarheid:
  - Log informatie centraal opslaan;
  - Back-up nemen van logbestanden;
  - Logging opnemen in DRP (disaster recovery plannen).

Ook over loggen moet worden gelogd: het openen van een nieuw logbestand, het verplaatsen, wijzigen naam of verwijderen van een logbestand, het inkijken, verwijderen of wijzigen van de inhoud van een logbestand dient te worden gelogd om niet-geautoriseerde toegang te kunnen opsporen.

Speciale aandacht moet besteed worden aan manuele logboeken omdat het risico op schending van vertrouwelijkheid, integriteit en beschikbaarheid groter zijn dan bij geautomatiseerde logging:

- Door de manuele procedure en opvolging is het risico op fouten, inconsistenties, ontbreken van informatie groter;
- Fysieke toegang tot het logboek moet beveiligd worden;
- Beschikbaarheid van het logboek moet gegarandeerd worden, bvb door het nemen van kopieën.

Mitigerende maatregelen om manuele logboeken te beveiligen bestaan o.a. uit:

- Fysieke toegangsbeveiliging d.m.v. afsluitbare/brandveilige kast;
- Kopieën bijhouden van het logboek;
- Inscannen en opslaan als pdf-bestand;
- Controle en 4-ogen principe.

Omgaan met fouten in auditing

Om te garanderen dat audit informatie steeds voorhanden is, is het belangrijk dat fouten tijdens de logging tijdig worden opgespoord en verholpen. Daarom moet logging zodanig opgezet worden dat geautoriseerd personeel automatisch op de hoogte wordt gebracht van problemen met het aanmaken en beheren van log informatie. De nodige aandacht moet gaan naar opslagcapaciteit voor logbestanden.

Als er niet meer gelogd kan worden, kan niet meer worden aangetoond wie toegang heeft gehad tot een systeem of tot informatie, of berichten ontvangen of verzonden zijn, of dat gegevens zijn ingevoerd en door wie. Dit brengt risico's voor de informatieveiligheid met zich mee.
De volgende keuzes moeten gemaakt worden:

- Het systeem of de toepassing normaal te laten functioneren en geen logging opslaan met als gevolg dat de log informatie verloren gaat.
- Het systeem of de toepassing lokaal te laten loggen en later de logging te synchroniseren. Veel systemen/toepassingen kunnen lokaal loggen, waardoor de log informatie tijdelijk wordt veiliggesteld. Op het moment dat het centrale logmechanisme weer beschikbaar komt, worden de verzamelde records alsnog doorgestuurd. Er moet wel over gewaakt worden dat de lokale logging niet alle beschikbare opslagcapaciteit van het systeem verbruikt. Op het moment dat de lokale opslag volloopt, moet opnieuw besloten worden of men in productie blijft of niet.
- Het systeem of de toepassing uit productie te nemen. Dit betekent dat gebruikers niet meer kunnen werken. Stoppen met verwerking betekent dat inbreuken niet ongemerkt kunnen plaatsvinden en ook dat de audit log geen hiaten gaat vertonen, maar dit gaat ten koste van de operationele werking.

Audit opvolging, analyse en rapportering

Log bestanden moeten regelmatig geanalyseerd worden om:

- Afwijkingen op beleidslijnen te detecteren,
- Ongewone activiteiten op te sporen en op te volgen,
- De effectiviteit van veiligheidsmaatregelen te testen.

Omdat log bestanden zeer veel informatie bevatten, is het ondoenbaar en inefficiënt om audit logs manueel na te kijken; er moeten dus geautomatiseerde tools geïmplementeerd worden om auditing, monitoring, analyse en rapportering in een coherent proces te verwerken.

Audit rapporten moeten periodisch aangemaakt worden en ter beschikking gesteld aan het management. Het is hierbij belangrijk dat de rapportering in begrijpelijke taal geschreven is, het mag dus niet alleen uit technische details bestaan.

Audit rapportering moet bovendien geïntegreerd worden in het proces voor incident- en probleem beheer.

Enkel geautoriseerd personeel mag audit rapporten aanmaken en reviewen.

2.2. Monitoring als maatregelen

Security monitoring bestaat uit het verzamelen en analyseren van informatie teneinde verdacht gedrag of niet-geautoriseerde toegang en activiteiten te detecteren, hierop alarmen te genereren en actie te ondernemen.

Een bijzondere vorm van security monitoring is SIEM: hierbij gaat men diverse bronnen raadplegen om op basis van deze informatie en de correlatie ervan verdacht gedrag of niet-geautoriseerde toegang en activiteiten te detecteren, hierop alarmen te genereren en actie te ondernemen.

Deze maatregelen onderscheiden zich van de logging als maatregelen door de nood aan gespecialiseerde tools en kennis om monitoring te kunnen implementeren. Als dusdanig worden ze dan ook voorzien als maatregel na risicoanalyse.

2.2.1. Security monitoring

Security Monitoring is een samenspel van mensen, processen en techniek. Er is techniek nodig om zichtbaar te maken wat erin gebeurt op gebied van informatie veiligheid. Daarna zijn er analisten nodig om gebeurtenissen te analyseren en om daar opvolging aan te geven.

Wat er precies door security monitoring wordt opgevolgd, wordt meestal bepaald door een risicoanalyse. Die risicoanalyse laat zien welke assets kritiek zijn en welke minder kritiek zijn. Aan de hand daarvan kan bepaald worden welke logging of alarmen relevante informatie kunnen opleveren rondom die assets. Als een risicoanalyse is uitgevoerd, kan er een kwalificatie toegekend worden aan de assets en bepaald worden wat wel en niet is toegelaten met die assets. De logging en alerting rond die assets en die van de maatregelen leveren relevante informatie op rondom de gebeurtenissen die plaatsvinden richting die assets. Een verzameling maatregelen en assets kunnen bijvoorbeeld zijn: een *active directory*, een firewall, een *intrusion detection* systeem, de antivirussoftware en de logging van de betrokken assets.

Security monitoring bestaat er dan verder in om de relevante informatie te verzamelen, te analyseren en op te volgen. Zo kunnen kwetsbaarheden, verdachte activiteiten en potentiële en

effectieve veiligheidsincidenten in het oog worden gehouden en waar nodig wordt dan actie genomen. Er kunnen ook trends geanalyseerd en gerapporteerd worden om preventieve acties te identificeren en in te plannen.

SIEM

Een SIEM oplossing biedt de mogelijkheid om informatie uit andere bronnen te gebruiken, bvb AD en e-mail logs, perimeter security logs, enz. Deze informatie wordt gebruikt om veiligheidsincidenten op te sporen. Het extraheren van incidenten uit logs is wat SIEM-systemen op een geautomatiseerde manier beloven te doen.

Een SIEM-oplossing voorziet in continu loggen en real-time monitoren van beveiligingsmaatregelen en alarmen veroorzaakt door afwijkend gedrag. Daarnaast wordt ook lange termijn opslag van log informatie en historische/trend analyses en koppeling met incident beheer en forensisch onderzoek.

SIEM is in feite samengesteld uit een aantal securityoplossingen:

- Log management: verzamelen en opslaan van log informatie van systemen en toepassingen;
- Security event management (SEM): real-time monitoring van gebeurtenissen rond informatieveiligheid;
- Security information management (SIM): legt zich toe op opslaan van informatie, analyse en rapportering;
- Security event correlatie (SEC): correlatie van de verzamelde informatie.

Vanuit diverse bronsystemen wordt informatie verzameld en verwerkt door de SIEM oplossing:

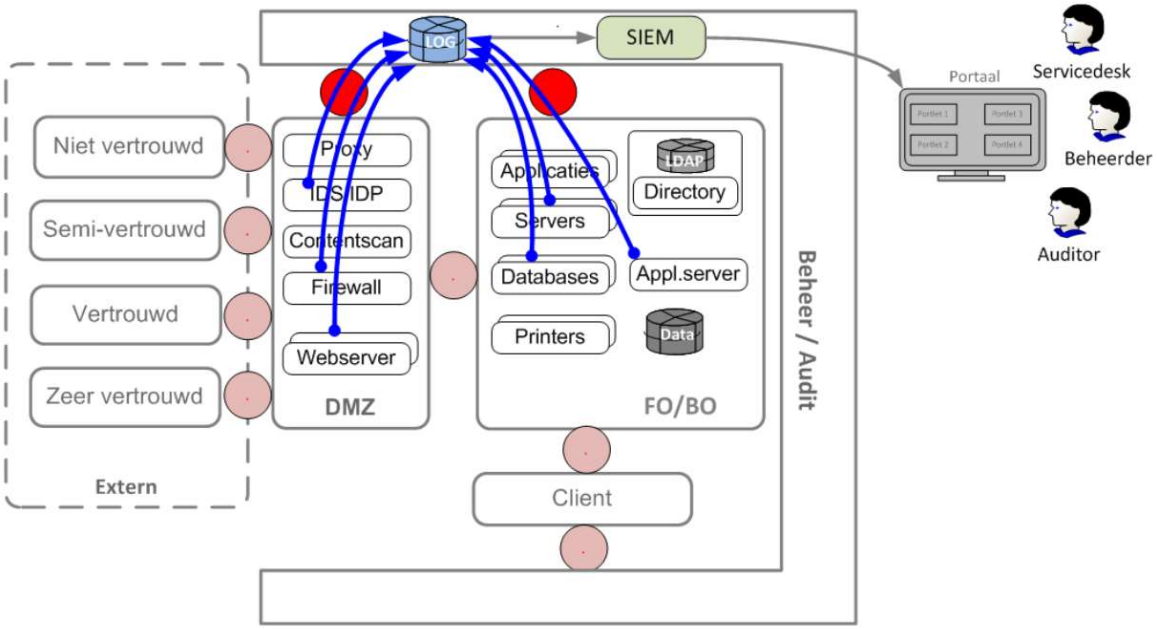
- Audit records worden verzameld uit de diverse bronsystemen,
- Audit records worden in een bepaald formaat gebracht voor verdere verwerking,
- De informatie wordt verrijkt vanuit andere bronnen (bv. AD voor linken van accounts aan gebruikersinformatie zoals naam, afdeling, locatie, …),
- Informatie wordt geaggregeerd en gecorreleerd,
- Analyse en rapportering.

Implementatie van een SIEM heeft de meeste toegevoegde waarde als aan twee voorwaarden is voldaan:

- Er moet een solide logging basis zijn,

Er moeten goede *use cases* uitgewerkt worden.

Een SIEM oplossing zou er bijvoorbeeld als volgt kunnen uitzien:



2.2.2. Logging in het kader van verwerking van persoonsgegevens

Logging en GDPR

Logging is een belangrijke maatregel ter ondersteuning van GDPR-conformiteit. Wanneer d.m.v. een systeem (toepassing, (gebruikers)apparatuur, server, database, …) toegang kan worden genomen tot persoonsgegevens, dan moet deze toegang gelogd worden. In GDPR vindt men dit terug als:

- **Logging als veiligheidsmaatregel**: artikel 24 – de verwerkingsverantwoordelijke moet de nodige technische maatregelen nemen om aan te kunnen tonen dat de verwerking in overeenstemming is met de Verordening.
- **Logging als middel voor transparantie**: artikel 13 en 14 – de betrokkene moet geïnformeerd worden over de categorieën van ontvangers van zijn gegevens en heeft het recht om te laten nagaan of de toegang door deze personen gerechtigd was of niet.
- **Logging als essentieel element in toegangsbeheer**: artikel 24 – logs worden ook gebruikt als intern controlemiddel.

Privacy logging

Privacy logs vereisen extra maatregelen tegenover ‘gewone’ security logging. Deze vereisten worden in dit hoofdstuk samengevat.

De GDPR stelt dat elke verwerking van persoonsgegevens gerechtvaardigd moet zijn. De privacy log dient dan ook een gepast antwoord op volgende vragen te geven:

- Wie heeft wanneer welke persoonsgegevens verwerkt[2]? Dit vertaalt zich naar een tot natuurlijke persoon herleidbare gebruikersnaam of ID, tijdsstip (datum/uur), identificatie van het werkstation of locatie, gebruikte toepassing.
- Wie is de betrokkene wiens persoonsgegevens werden verwerkt? Dit vertaalt zich naar de persoon die het object is van de handeling.
- Wat was het resultaat van deze verwerking? Dit vertaalt zich naar het resultaat van de handeling (consultatie, wijziging, verwijdering, query).

De privacy logs moeten bewaard worden overeenkomstig de toepasselijke wet- en regelgeving. Voor de KSZ is bvb een bewaartermijn van 10 jaar voorzien.

Aangezien de privacy logs evenzeer persoonsgegevens bevatten, moeten zij dezelfde informatieklasse toegewezen krijgen als de informatieklasse die aan de persoonsgegevens werd gegeven (informatieklasse 3 voor logbestanden op de verwerking van algemene persoonsgegevens, informatieklasse 4 voor logbestanden op de verwerking van gevoelige persoonsgegevens).

De integriteit van de logs moet bewaard worden zodat manipulaties vermeden worden en de consistentie in de loginformatie bewaakt wordt.

Logging inbreuken

De GDPR stelt in artikel 33: '*De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen*.'

Het bijhouden van een logboek met inbreuken in verband met de verwerking van persoonsgegevens is dan ook aangewezen. Dit logboek moet een antwoord bieden op volgende vragen:

- Wat is er gebeurd?
- Op welke datum en tijdsstip is de inbreuk vastgesteld?
- Welke persoonsgegevens zijn hierbij betrokken?
- Wie zijn de personen wiens gegevens betrokken zijn bij de inbreuk?
- Welke zijn de gevolgen voor de betrokkenen?
- Welke maatregelen worden genomen om de gevolgen van de inbreuk te verminderen?
- Welke maatregelen worden genomen om de inbreuk in de toekomst te voorkomen?

3. LINK MET ANDERE MAATREGELEN

SIEM is geen alleenstaand proces maar heeft interacties met de andere beheersprocessen:

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

De maatregel PAM of *Privileged Access Management* beschrijft hoe het gebruik van geprivilegieerde rechten zoals toegekend aan systeembeheerders, ontwikkelaars, … moet worden toegekend en opgevolgd. Het gebruik van logging voor geprivilegieerde rechten is in dit document opgenomen.

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

Logbestanden bevatten een groot scala aan informatie en moeten dus op hun beurt voldoen aan het informatieclassificatie model. Als gevolg daarvan is het denkbaar dat loginformatie informatieklasse 3 of hoger toegekend krijgt of dat er persoonsgegevens in de logbestanden opgeslagen worden, waardoor de maatregelen rond cryptografie zoals beschreven in het bovengenoemd document van toepassing zijn.

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

Logs bieden waardevolle informatie voor het inschatten van bedreigingen, hun waarschijnlijkheid en impact – en dus informatie voor het uitvoeren van risicoanalyses. Ze bieden namelijk inzicht in de reconstructie van reële incidenten en bedreigingen.

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

Loginformatie kan helpen bij het onderzoek van een incident. Belangrijk hierbij is dat enerzijds genoeg informatie gelogd wordt en anderzijds dat de loginformatie lang genoeg wordt bijgehouden om na een incident ver genoeg in de tijd te kunnen teruggaan voor de reconstructie van het incident.