UWV Richtlijn Logging en Monitoring voor IB&P
Versie 4.1

Inhoud

Documentgegevens

Documentinformatie

Naam	Richtlijn Logging en Monitoring
Datum	19-03-2018
Versienummer	4.1
Status	Concept
Classificatie	Vertrouwelijke informatie
Opdrachtgever	CISO
Auteur	Rob Roukens
Eigenaar	CISO

Versiebeheer

Versie	Datum	Wijzigingen	Distributie	Besluit
0.1	25-05-2015	1ste concept		
0.2	12-06-2015	2de concept	SOC, IS	
0.5	17-07-2015	Commentaar SOC, IS verwerkt.	C-IB&P	Ter review aanbieden aan de C-IB&P
0.6	09-09-2015	Commentaar C-IB&P verwerkt	CISO	Aanpassen
0.7	29-12-2015	Toevoegen risk based, bewaartermijnen en meldplicht	CIOO	Aanpassen
0.8	28-01-2016	Commentaar CIOO verwerkt	CIOO	Akkoord
0.8	02-02-2016	Review Business gevraagd	Coordinatoren IB&P	Commentaar verwerken
4.0	08-04-2016	Commentaar verwerkt	AB	Definitief
4.1	19-03-2018	Input vanuit evaluatie LoMo realisatie en toetsing AVG	Tactische Coalitie / AB	

1. Inleiding

Het doel van dit document is om invulling (richtlijnen) voor het beleid (BIR) te geven, gebaseerd op risico-inschatting voor logging en monitoring van systemen en gegevens binnen de bedrijfsprocessen van UWV.

Deze richtlijn is een actualisatie van het UWV-beleidsdocument "Logging en Monitoring V4.0 dd 08-04-2016" en dekt naast de eisen uit de BIR UWV ook de eisen uit andere relevante regelgeving[1] op dit vlak af. Alle voor UWV relevante eisen ten aanzien van beveiligingsgerelateerde logging en monitoring worden dan ook benoemd in deze richtlijn.

1.1. Aanleiding

UWV vervult een belangrijke maatschappelijke en economische functie in onze samenleving. Als bewaarder en behandelaar verzamelen, verwerken en versturen wij een grote diversiteit en complexiteit aan gevoelige informatie. Als beheerder of eigenaar van deze informatie is het onze plicht om dit op een uiterst zorgvuldige, betrouwbare en veilige wijze te doen. Bovendien wordt UWV in toenemende mate blootgesteld aan externe dreigingen en geldt er strengere wet- en regelgeving. Logging en monitoring is een van de maatregelen die bijdraagt aan het beveiligen van onze informatie en informatiesystemen.

1.2. Scope

De eisen gelden voor alle informatiesystemen en processen die onder de verantwoordelijkheid van UWV vallen en waarvoor zij het functioneel beheer uitvoert. Het perspectief is dat van informatiebeveiliging, en daarmee het voorkomen en opsporen van, en het reageren op bedreigingen voor onder andere de systemen, processen en gegevens van de organisatie.

Deze richtlijn geeft invulling aan de volgende maatregelen voor technische logging en auditlogging: (zie Borging BIR Beheersing voor verantwoordelijkheden)

1. Uit de BIR UWV:
- 10.6.1 Maatregelen voor netwerken;

[1] Relevante regelgeving wordt benoemd in § 1.2 en Bijlage C Bronnen,

- 10.10.1 Aanmaken audit-logbestanden;
- 10.10.2 Controle van systeemgebruik;
- 10.10.3 Bescherming van informatie in logbestanden;
- 10.10.4 Logbestanden van administrateurs en operators;
- 10.10.5 Registratie van storingen;
- 10.10.6 Synchronisatie van systeemklokken.

2. Uit de Beveiligingsrichtlijnen webapplicaties deel 2 van het NCSC:
- C06 Logging;
- C07 Monitoring.

3. Uit richtsnoeren beveiliging persoonsgegevens van het AP:
- Logging en controle.

4. Uit SSD-beveiligingseisen v 2.0: normen 9 en 30 (Inlog- en Applicatielogging).
5. Uit Logius richtlijnen: B7-8
6. Algemene Verordening Gegevensbescherming artikel(en): Art. 32, lid 1; Art. 5, lid 1, sub f.
7. UWV Juridisch Kader Logging & Monitoring

Niet in scope is het monitoren op dreigingen vanuit (externe) leveranciers. Hiervoor zijn aparte contracten afgesloten en controle vindt via audits/assuranceonderzoeken plaats.

1.3. Leeswijzer

Hoofdstuk 2 beschrijft de achtergrond en visie over logging en monitoring. Hoofdstuk 3, 4 en 5 beschrijven achtereenvolgens de regelgeving voor logging, monitoring en SIEM. Hoofdstuk 6 beschrijft het realisatieproces.

In bijlage A staan de definities van de conformiteitsindicatoren. Bijlage B geeft een toelichting op de SIVA-methodiek. In de SIVA-methodiek wordt per norm kort aangegeven wat de onderbouwing voor de norm is, met een voorstel voor de te implementeren maatregelen. In bijlage C is een overzicht van brondocumenten opgenomen alsmede een afkortingenlijst. In bijlage D treft men de te hanteren sjablonen aan die gebruikt kunnen worden in het realisatie- en monitoringproces.

2. Achtergrond

Het breder en intensiever inzetten van e-dienstverlening, mobiele apparaten en telewerken stelt UWV in staat aan te sluiten bij de hedendaagse eisen van medewerkers en klanten. Tegelijkertijd zijn de bedreigingen vanuit de buitenwereld zowel als van binnenuit toegenomen. Het gevolg van deze twee ontwikkelingen is dat de beveiligingsrisico's voor UWV groter zijn geworden, waardoor er meer kans is op schade voor burgers (privacyschending), bedrijven en de reputatie van UWV zelf. Daarnaast zijn wet- en regelgeving en de verplicht te hanteren externe normen op het gebied van beveiliging en monitoring aangescherpt. Zo moet in het kader van AVG het principe Privacy by design/Privacy by default gehanteerd worden. Gezien bovengenoemde ontwikkelingen is het daarom noodzakelijk om ook het informatiebeveiligingsbeleid en de - richtlijnen aan te scherpen en te implementeren.

2.1. Definities

Logging: Het proces van registreren van informatie (voor Informatie Beveiliging & Privacy (IB&P) analyse en bewakingsdoelstellingen) over menselijke- en systeemactiviteiten binnen systemen en op netwerken van UWV, en het vastleggen daarvan in logrecords.

Monitoring: Het gebruiken van gelogde informatie om de digitale veiligheid van de organisatie en de privacy van de burger te waarborgen.

Informatiesysteem: Wordt in brede zin gebruikt en kan zowel verwijzen naar applicaties en databases in de bedrijfsvoering als naar middlewarepakketten en infrastructuurcomponenten.

Vertrouwelijkheidsklasse: Dit is de maat voor het bepalen van de waarde van -, de wettelijke eisen aan - en de gevoeligheid van gegevens. De bepaling van de vertrouwelijkheidsklasse is nodig voor het treffen van een passend beveiligingsniveau bij de gegevens[2].

Integriteitsklasse
De maat voor het bepalen van de waarde van de juistheid, tijdigheid, actualiteit en volledigheid van informatie en de verwerking daarvan.

SIEM (soms onderdeel van Loghost): De term ***S***ecurity ***I***nformation and ***E***vent ***M***anagement staat voor een appliance met mogelijkheden van het verzamelen, analyseren en presenteren cq rapporteren van (logging)informatie.

Logstore (centrale loggingopslag (nog niet operationeel bij UWV))
Een centrale opslagvoorziening voor logdata ten behoeve van een SIEM of Loghost (forensische) analyses of audittrails door andere toepassingen. In de regel wordt hierbij een langere bewaartermijn gehanteerd dan bij de door het SIEM verwerkte logdata.

Informatiebeveiligingsgebeurtenis
In het kader van logging en monitoring betreft het hier een gebeurtenis (vaak een dreiging die manifest wordt) die middels logging en monitoring kan worden gedetecteerd en gerapporteerd.

2.2. Doelen van logging en monitoring

Van logging en monitoring kunnen twee kerndoelstellingen onderkend worden:

1. *Bewaken van de integriteit*: Het is voor de bedrijfsvoering van UWV essentieel dat schending van gevoelige gegevens en schade aan (de prestaties van) systemen zo veel mogelijk voorkomen wordt. Daarom is het cruciaal dat de correctheid, beschikbaarheid en stabiliteit van deze middelen gemonitord wordt, zodat waar nodig correctieve maatregelen genomen kunnen worden.
2. *Bewaken van de vertrouwelijkheid van gegevens*: UWV bezit en gebruikt veel privacy-gevoelige gegevens en moet hier op een vertrouwelijke wijze mee om gaan. Zowel voor UWV-medewerkers als voor andere stakeholders gelden strikte eisen ten aanzien van doelbinding en proportionaliteit. Op deze manier moet voorkomen worden dat gegevens misbruikt worden, bijvoorbeeld door het plegen van fraude, het lekken van persoonsgegevens of onbevoegde raadpleging. Logging kan helpen gebruikersgedrag te registreren, zowel voor de actieve 'dagelijkse' monitoring (realtime of achteraf) als voor het passief bewaren van audit trails t.b.v. onderzoek (Logstore).

[2] Zie voor details de Richtlijn Classificatie voor Vertrouwelijkheid v1.0

Deze twee kerndoelstellingen van logging en monitoring moeten onder meer helpen meer strategische achterliggende doelen te bereiken zoals het voorkomen van juridische procedures, Kamervragen en reputatieschade. Een goede bedrijfsvoering houdt in dat UWV zich aan de wet en aan maatschappelijke normen en waarden houdt, zeker gezien het feit dat de organisatie een kwetsbare reputatie heeft.

Logging en monitoring zijn twee elementen van een bredere strategie om de informatie(systemen) binnen een organisatie te beveiligen. Andere elementen zijn bijvoorbeeld bewustwordings-campagnes en rol gebaseerde autorisatie. Bedreigingen kunnen zich manifesteren in technische vorm (bijvoorbeeld via virussen en trojans) en via het gedrag van interne medewerkers en externe portaalbezoekers. Logging en monitoring zijn echter van groot belang om beveiligingsincidenten en structurele zwaktes te identificeren. Zo kunnen met behulp van logging en monitoring urgente gevallen opgelost worden en kan de complete beveiliging naar een hoger niveau worden getild.

Om bovengenoemde twee doelen te behalen, dienen de volgende zaken op basis van een risicoafweging, zoals bijvoorbeeld is toegepast om te komen tot de BIR UWV lijst, goed ingeregeld te zijn. Beide zaken dienen zowel doel 1 als 2.

a. *Vastlegging van audit trails en user accounts*: Dit zorgt ervoor dat (trans)acties en autorisaties te analyseren en te herleiden zijn naar specifieke gebruikers, objecten en systemen. Dit is een wettelijke vereiste ten aanzien van onweerlegbaarheid. Deze zorgt er dus voor dat er achteraf incidentanalyses (o.a. reconstructie van gebruikerspaden) kunnen worden uitgevoerd indien daar reden voor is. Deze incidentanalyses kunnen worden gebruikt in eventuele bewijsvoering. De user accounts betreffen zowel interne UWV-medewerkers als externe accounthouders (waaronder portaalbezoekers).

b. *Signalering van ongewenste situaties*: Een goede monitorvoorziening zorgt ervoor dat verdachte gedragingen ontdekt worden, bijvoorbeeld door te kijken naar patronen in gelogde gebeurtenissen. Denk hierbij aan het detecteren van afwijkingen van normale situaties en het herkennen van vooraf gedefinieerde bedreigingen. Dit kan vereisen dat 'normale situaties' eerst worden gedefinieerd (denk aan doorsnee gedrag dat blijkt uit audit trails, gemiddeld aantal raadplegingen van persoonsgegevens in een applicatie of gemiddelde aantallen portaalbezoekers of modale performance niveaus).

Het type beveiligingsmaatregel bepaalt de rol die logging en monitoring kan spelen:

Type maatregel	Omschrijving	Rol van logging en monitoring
Afschrikking	Het voorkomen dat partijen bedreigende acties ondernemen, bijvoorbeeld via bewustwordingsprogramma's die het beleid en de mogelijke straffen communiceren.	De wetenschap dat er scherp gelogd en gemonitord wordt kan vooral interne medewerkers ervan weerhouden ongewenste gegevensbevragingen en –bewerkingen uit te voeren.
Preventie	Het voorkomen dat partijen die bedreigende acties ondernemen deze ook daadwerkelijk ten uitvoer kunnen brengen. Bijvoorbeeld door wachtwoorden, rol gebaseerde autorisatie, IDS en versleuteling.	Een SIEM bevat een Intrusion Detection System (IDS = real time monitoring) en levert input voor verdere analyse.
Detectie	Het (vaak achter af) ontdekken van uitgevoerde bedreigende acties en pogingen daartoe.	Dit is het primaire doel van logging en monitoring.
Correctie	Het herstellen van de negatieve effecten. Dit kan een direct herstel zijn van de schade, een bekrachtiging van het beleid (bijvoorbeeld het straffen van een dader), of het bijwerken van het beveiligingsbeleid.	Bijvoorbeeld het middels audit trails bewijzen van overtredingen of het waarschuwen van medewerkers als ze mogelijk de regels hebben overtreden.

Tabel 1: Rol van logging en monitoring per type maatregel

2.3. Compliance bij risicogestuurd beveiligen als leidraad bij aansluiting op SIEM

Het doel van de middels risicoanalyse vastgestelde BIR-RAL (Risico Applicatie Lijst) is om UWV-breed inzichtelijk te maken welke applicaties het meest risicovol zijn. Dit bezien vanuit de door de RvB vastgestelde top 4 risicoclusters (zie hieronder). De risicoclusters zijn vertaald naar een set aan vragen/indicatoren, waaraan vervolgens een wegingsfactor is toegekend. Dat leidt tot een risico indicatie getal per applicatie. De opzet van de inventarisatie is afgestemd met de CISO, het USOC en de AD. Van de meest risicovolle applicaties dient een afweging (comply or explain, zie hieronder) gemaakt te worden of aansluiting op het SIEM een passende beveiligingsmaatregel is.

risicocluster 1: Digitale dienstverlening aan de burger.

risicocluster 2: Gegevensuitwisseling met andere partijen.
risicocluster 3: Interne toegang tot systemen inclusief de bijbehorende mensaspecten.
risicocluster 4: Overig.

2.4. Afwijkingen via 'Comply or Explain'

De gestelde richtlijnen voor logging en monitoring zijn normatief en daarmee kader stellend (dus bindend).

De gestelde criteria zijn *Principle Based*. Afwijkingen van deze richtlijn moeten worden gemotiveerd volgens het 'comply or explain' principe, waarbij de inherente risico's aantoonbaar worden afgewogen en de verantwoordelijke lijnmanager tekent voor de restrisico's. De verantwoordelijke eigenaar van de IT-middelen of ondersteunende processen ziet toe op naleving van de 'comply or explain' van deze richtlijn.

2.5. Bewaartermijnen logs

Voor logbestanden die alleen bedoeld zijn voor IB&P-doeleinden, zoals in dit document beschreven, geldt een bewaartermijn van 1 jaar. In het geval dat er sprake is van het feit dat deze gegevens gebruikt zijn voor een (forensisch) onderzoek dan moeten deze gegevens 10 jaar worden bewaard.

Binnen UWV zijn ook andere wetten, o.a. archiefwet, van toepassing waarin bewaartermijnen worden genoemd, ter informatie:

- loggegevens met betrekking tot financiële afhandeling moeten 7 jaar worden bewaard;
- logggegevens in het kader van inzage en correctierecht met betrekking tot een claimdossier wordt volgens de huidige geldende selectielijsten 5 jaar bewaard;
- en als het een medisch dossier betreft 10 jaar.

Bij de bepaling van een bewaartermijn speelt het proces waarin de loggegevens worden gebruikt een cruciale rol. Het kan zo zijn dat bepaalde loggegevens in meerdere afzonderlijke processen worden gebruikt. In dat geval geldt de langste bewaartermijn. De bewaartermijnen die UWV hanteert zijn vastgelegd in een selectielijst (zie intranetpagina DIV), die verplicht is op grond van artikel 5 van de Archiefwet 1995.

2.6. Systeemeigenaar versus gegevenseigenaar

De systeemeigenaar is verantwoordelijk voor zijn/haar dreigingen ten aanzien van het syteem en heeft een verantwoordelijkheid t.a.v. de business(proces)gegevens van andere organisatieonderdelen in zijn/haar systeem. De systeemeigenaar is te allen tijde eigenaar van de logdata die wordt gebruikt voor alle use cases die voortkomen uit zijn/haar systeem.

Er kunnen twee stuaties ontstaan:

1 De use cases van de systeemeigenaar komen overeen met de use cases van de gegevenseigenaar van de gegevens waarover de use cases gaan.
In dit geval kan logdata worden aangeleverd aan de monitoringtool waarbinnen een rapportage naar kostenplaats over dezelfde use cases plaatsvindt aan alle eigenaars.

2 De use cases van de systeemeigenaar komen niet overeen met de use cases van de gegevenseigenaar van de gegevens waarover de use cases gaan.
In dit geval dient de gegevenseigenaar (=de risicodragende partij) een verzoek bij de systeemeigenaar in te dienen om de noodzakelijke aanpassingen te doen zodat de loggegevens aan de monitoringtool kunnen worden verstrekt. Rapportage vindt vervolgens alleen aan gegevenseigenaar plaats (dus niet aan systeemeigenaar).
De systeemeigenaar kan de kosten van de noodzakelijke aanpassingen verhalen op de gegevenseigenaar.

3. Logging

3.1. Inleiding

Dit hoofdstuk geeft een opsomming van de beveiligingscriteria (principes of hoofdnormen) en maatregelen voor logging.

Voor de criteria en maatregelen geldt:

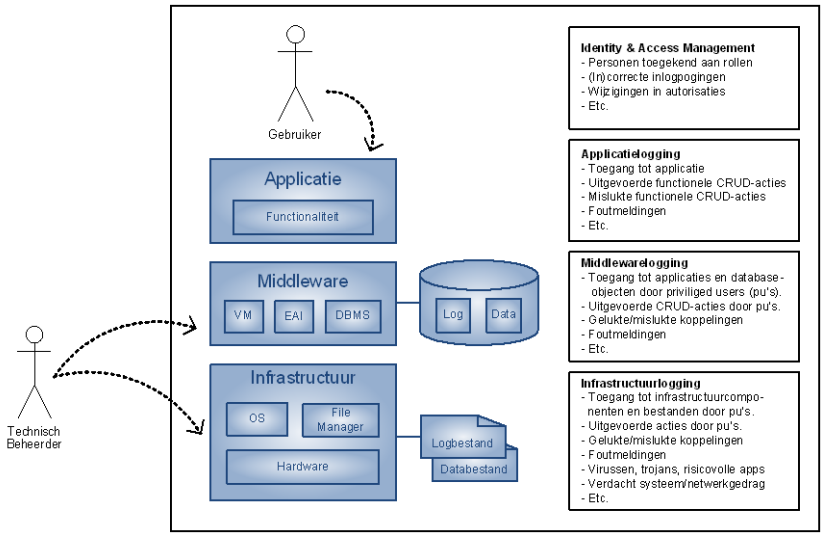
- De criteria zijn randvoorwaarden waaraan **moet** worden voldaan. Indien niet wordt voldaan aan gestelde criteria moet de afwijking worden toegelicht conform het *Comply or Explain* principe;
- De genoemde maatregelen zijn Best Practice maatregelen die invulling te geven aan het bovenliggende criterium;
- De criteria en maatregelen sluiten aan bij de UWV BIR en de andere genoemde wet en -regelgeving uit paragraaf 1.1.

In de volgende paragraaf zijn de criteria **Registreren audit- logbestanden** en **Beveiliging van informatie in logbestanden** nader toegelicht en voorzien van maatregelen.

3.2. Typen logbestanden

Figuur 1 laat zien dat er verschillende lagen in logging en monitoring aanwezig zijn. De gebruiker maakt louter gebruik van de applicatie om functionele acties uit te voeren (bijvoorbeeld het lezen en bijwerken van gegevens van uitkeringsgerechtigden).

Een functioneel beheerder die via de applicatie loginformatie bekijkt is in dat geval simpelweg een reguliere gebruiker. Een Technisch Beheerder heeft toegang tot de objecten waar de applicatie mee werkt (bijvoorbeeld databasetabellen of bestanden), maar kan dit buiten de applicatie om doen. De acties van beide typen gebruikers dienen gelogd te worden, waarbij het monitoren van de acties van de technisch beheerder (externe leverancier) buiten scope van deze richtijn vallen aangezien de monitoring hiervan middels contracten is geregeld met de beheerpartij.



Figuur 1. Logging per laag

Desbetreffende patronen van afwijkend en opmerkelijk gedrag kunnen op alle lagen worden gedefinieerd. De middleware en infrastructuurlagen kunnen daarnaast – als gevolg van hun generieke aard – ook gebruik maken van door de industrie gedefinieerde 'signatures' en virusdefinities die wijzen op bedreigende situaties.

De lagen laten zien dat logging verticaal gekoppeld kan worden, bijvoorbeeld in een keten. Echter, applicaties en andere lagen kunnen ook horizontaal gekoppeld worden. Zo ontstaat Logging en monitoring over de keten (horizontaal of verticaal), dit kan nodig zijn om specifieke dreigingen te kunnen detecteren.

3.3. Maatregelen voor Logging

LM01 – Logging – Registreren audit- logbestanden		
Criterium (wie en wat)	Van informatiebeveiligingsgebeurtenissen dient een minimale set gegevens van benoemde gebeurtenissen te worden vastgelegd in audit-logbestanden, deze worden periodiek beoordeeld en gedurende een overeengekomen periode bewaard (zie bewaartermijnen) ten behoeve van toekomstig onderzoek en toegangscontrole.	BIR 10.10.1, 10.10.2 en 10.10.4
Doelstelling (waarom)	Met zekerheid kunnen detecteren van eventuele schendingen van functionele of beveiligingseisen en om achteraf de juistheid van uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Risico	Schendingen kunnen niet gesignaleerd worden en herstel acties kunnen niet tijdig worden genomen wat tot (reputatie) schade voor het UWV kan leiden	

Maatregelen

Minimale set gegevens		
01	Een regel uit een audit-logregel dient minimaal de volgende gegevens te bevatten: • een tot een natuurlijk persoon (zoals gebruiker, systeemadministrator of systeemoperator) herleidbare gebruikersnaam of ID; • de gebeurtenis/handeling • de identiteit van het werkstation of de locatie; • het object waarop de handeling werd uitgevoerd (bijvoorbeeld een natuurlijk persoon en het burgerservicenummer); • het resultaat van de handeling; • de datum en het tijdstip van de gebeurtenis.	BIR 10.10.1.2 10.10.4.1
02	In een logregel dienen in principe geen gevoelige gegevens te worden opgenomen. Dit betreft ondermeer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers etc).	BIR 10.10.1.3
03	Logging dient beperkt te blijven tot de gegevens die noodzakelijk zijn voor de detectie van de dreigingen tegen de realisering van de vooraf gestelde proces- en systeemdoelen onder doelbinding en proportionaliteit.	Richtsnoeren AP

Benoemde gebeurtenissen		

04	De volgende beveiligingsgebeurtenissen dienen in ieder geval te worden opgenomen in de logging:
	• het optreden van beveiligingsincidenten t.a.v. de infrastructuur zoals
	  ○ het vaststellen van de aanwezigheid van malware,
	  ○ het constateren van vulnerabilities,
	  ○ het optreden van verstoringen in het productieproces zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen;
	• het optreden van business beveiligingsincidenten t.a.v. applicaties zoals
	  ○ gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuraties en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases);
	  ○ foutieve inlogpogingen c.q. geweigerde pogingen om toegang te krijgen,
	  ○ overschrijding van autorisatiebevoegdheden of het verkrijgen van ongeautoriseerde toegang tot persoonsgegevens,
	  ○ activiteiten die gebruikers uitvoeren met persoonsgegevens;
	  ○ handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, direct gebruik van online transacties (ook A2A koppelingen) en toegang tot bestanden buiten de reguliere applicaties om.
	• Het optreden van beheersbeveiligingsincidenten zoals:
	  ○ uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore;
	  ○ handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels;
	  ○ het plotselinge starten van (tot dan toe) niet operationele systeemservices,
	  ○ het starten en stoppen van security services;
		BIR 10.10.2.1 10.10.5.1
		
		NSCS C.06.1
		
		SSD 30/01.02
		
		Richtsnoeren AP

Bewaard		
07	De beschikbaarheid van loginformatie dient gewaarborgd te zijn binnen de termijn waarin loganalyse noodzakelijk wordt geacht, max 1 jaar. Bij een informatiebeveiligingsincident is de bewaartermijn 10 jaar. De bewaartermijnen dienen tot uitdrukking te komen in de configuratie instellingen van de systemen.	BIR 10.10.3.5 NSCS C.06.6 SSD 30/03.02
08	Na het verstrijken van de bewaartermijn (zie 2.5) moeten de logs gewist en/of de drager van de logregistratie vernietigd worden. Dit dient op een zodanige wijze te gebeuren dat reproductie niet mogelijk is en bewijs van vernietiging voorhanden is.	

Toelichting op maatregelen

02 *Als het toch noodzakelijk is om gevoelige (persoons)gegevens in een log regel op te nemen bijvoorbeeld omdat het een sleutelgegeven is van een gemuteerd record, dan moeten er adequate extra beveiligingsmaatregelen t.a.v. de vertrouwelijkheid worden genomen (zie LM02)*

03 *Loginformatie ten aanzien van handelingen met (strikt)vertrouwelijke (persoons)gegevens is noodzakelijk om aan wetgeving te voldoen, zoals bepaling doelbinding.*
Richt risicomanagement in om vast te stellen m.b.t. welke gebeurtenissen en handelingen log gegevens moeten worden vastgelegd.

04 *Regelmatig de alerts en logs en bijbehorende overzichten in de gaten houden zorgt er niet alleen voor dat specifieke incidenten worden gedetecteerd en opgepakt, maar ook dat er kennis over het gebruik van het systeem ontstaat, wat weer input vormt voor de bepaling van wat 'normaal' en wat 'verdacht' gedrag is.*
De regels voor afgeven van alerts en de inrichting van de rapportages dienen regelmatig (jaarlijks of eerder indien aanleiding) te worden herijkt o.b.v. opgedane ervaringen.

07 *Indien er bijzondere redenen zijn om een langere of kortere bewaartermijn te hanteren, dan moet dat expliciet worden gemaakt.*

LM02 – Logging – Beveiliging van informatie in logbestanden		
Criterium (wie en wat)	De informatie in logbestanden dient te worden beveiligd tegen inbreuk en verstoring en tegen onbevoegde toegang.	BIR 10.10.3 10.10.5 en 10.10.6
Doelstelling (waarom)	Zorg dragen dat het mogelijk blijft om (achteraf) met zekerheid eventuele schendingen van functionele en beveiligingseisen te detecteren en aantonen.	

LM02 – Logging – Beveiliging van informatie in logbestanden	
Risico	Er bestaat geen zekerheid of schendingen correct zijn gesignaleerd en welke herstel acties dienen te worden genomen. Logbestanden waarop mogelijk integriteitsinbreuk is gepleegd kunnen niet meer dienen als bewijsmateriaal bij incidenten.

Maatregelen

Inbreuk en verstoring		
01	Het (automatisch) overschrijven of verwijderen van logbestanden dient te worden gelogd in een separaat aan te leggen logbestand.	BIR 10.10.3.1
02	De opslag van logging dient te worden gecontroleerd: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens dient te worden gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).	BIR 10.10.1.5 en 10.10.3.6
03	De instellingen van logmechanismen dienen zodanig te worden beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden dient daarbij altijd het vier ogen principe toegepast te worden.	10.10.3.4
04	Om een betrouwbare analyse van logbestanden mogelijk te maken dienen de systeemklokken van alle relevante informatiesystemen te worden gesynchroniseerd met een nauwkeurige tijdsbron.	BIR 10.10.6.1 NSCS C.06.4 SSD 30/02.01
Beveiligd		
05	Er dient vooraf bepaald te zijn wat te doen bij het uitvallen van logging mechanismen (alternatieve paden).	NSCS C.06.5 SSD 30/03.01
Onbevoegde toegang		
06	Het raadplegen van logbestanden dient voorbehouden te zijn aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.	BIR 10.10.3.2
07	Logbestanden dienen zodanig beschermd te zijn dat deze niet aangepast of gemanipuleerd kunnen worden zodat de ontvangende (controlerende) partij de integriteit van de logbestanden kan vaststellen.	BIR 10.10.3.3 NCSC C.06.7 SSD 30/03.03

Toelichting op maatregelen

04 *Gesynchroniseerde systeemklokken zijn essentieel om afzonderlijke logbestanden aan elkaar te relateren bv. correlatie bij onderzoek van een incident over een systeemketen heen.*
Systemen gebruiken interne systeemklokken voor "time stamps" bij het vastleggen van loggegevens. In ontwerp- of configuratiedocumentatie is vastgelegd hoe het synchroniseren van de systeemklokken is geconfigureerd.

05 *Er wordt aangegeven welke actie een component neemt op het moment dat het centrale loggingsmechanisme niet meer beschikbaar is. Er is een procedurebeschrijving van het loggingmechanisme en bewijsvoering dat het mechanisme van alternatieve actie bij uitvallen loggingsmechanismen ook daadwerkelijk werkt.*

07 *Logs die persoonsgegevens (o.a. user ID's) bevatten moeten als vertrouwelijk worden behandeld, terwijl logs die onderzoek ondersteunen beschermd moeten worden tegen vernietiging of aanpassing.*
Ontwerpdocumentatie en configuratie stellingen en autorisatieprofielen geven aan hoe logfiles beschermd zijn.

4. Monitoring

4.1. Inleiding

Dit hoofdstuk geeft een opsomming van de beveiligingscriteria (principes of hoofdnormen) en maatregelen voor monitoring.

Voor de criteria en maatregelen geldt:

- De criteria zijn randvoorwaarden waaraan moet worden voldaan. Indien niet wordt voldaan aan gestelde criteria moet de afwijking worden toegelicht aan de Business Security Officer, conform het *Comply or Explain* principe. Een afwijking (*Explain*) kan bijvoorbeeld zijn ingegeven door een risico-analyse;
- De genoemde maatregelen zijn *Best Practice* maatregelen die invulling te geven aan het bovenliggende criterium;
- De criteria en maatregelen sluiten aan bij de UWV BIR en de andere genoemde regelgeving uit paragraaf 1.1.

In de volgende paragraaf zijn de criteria voor **Monitoring van netwerken** en **Monitoring bewaken** nader toegelicht en voorzien van maatregelen.

4.2. Maatregelen voor Monitoring van beveiligingsincidenten

LM03 – Monitoring van Infrastructuur, Middleware en applicaties		
Criterium (wie en wat)	IT middelen (Infrastructuur, waaronder ook netwerken, middleware en applicaties) behoren adequaat te worden gemonitord om ze te beschermen tegen bedreigingen en om beveiliging te handhaven.	BIR 10.6.1 Richtsnoer AP etc
Doelstelling (waarom)	De inrichting van de IT-middelen en de gehanteerde protocollen dienen aanvallen/dreigingen te detecteren om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Risico	Via technische componenten van IT middelen wordt vertrouwelijkheid, integriteit en/of beschikbaarheid aangetast, zonder dat dit (tijdig) gedetecteerd wordt en zonder dat hierop geacteerd kan worden.	

Maatregelen

Monitoren		
01	Het netwerk dient te worden gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimumniveau komt.	BIR 10.6.1.1
02	De eigenaar van de IT middelen dient een proces in te regelen dat op heldere en expliciete wijze riskbased monitoring en bijbehorend incidentmanagement garandeert.	

LM04 – Monitoring bewaken		
Criterium (wie en wat)	De logging- en detectie informatie (registraties en alarmeringen) en de condities van de beveiliging van IT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	NCSC C.07
Doelstelling (waarom)	Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de IT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Risico	Onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.	

Maatregelen

01	De door verschillende beheerdisciplines gelogde informatie dient voor analysedoeleinden centraal te worden samengebracht.	NCSC C.07.1 SSD-30/01.01
02	Periodiek dienen actief compliance controles uitgevoerd te worden op: • wijzigingen aan de configuratie van (web)applicaties; • optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; • ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.	NCSC C.07.3
03	Er dienen periodieke reviews van acces logs te worden uitgevoerd.	NCSC C.07.4
04	Log bestanden inzake beveiligingsgebeurtenissen dienen na ontvangst te worden gecontroleerd op indicaties van onrechtmatige toegang tot of onrechtmatig gebruik van persoonsgegevens waarop waar nodig actie dient te worden ondernomen.	Richtsnoeren AP
05	Van log bestand controles dienen rapportages te worden gemaakt die minimaal maandelijks worden beoordeeld.	BIR 10.10.1.1
Analyseren (auditing)		
06	De verzamelde loggingsinformatie dient in samenhang te worden geanalyseerd.	NCSC C.07.5
07	Periodiek dienen de geregistreerde menselijke en systeemacties te worden geanalyseerd.	NCSC C.07.6
08	Periodiek dient een analyse uitgevoerd te worden op ongebruikelijke situaties (incidenten) die de werking van (web) applicaties kunnen beïnvloeden.	NCSC C.07.7
Rapporteren (alerting)		
09	Periodiek dienen de resultaten van geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management te worden gerapporteerd.	NCSC C.07.8
10	De rapportages uit de beheerdisciplines compliance management, vulnerability assessment, penetratietest en logging en monitoren worden door het UWV SOC geanalyseerd en geëvalueerd op aanwezigheid van structurele risico's. De resultaten hieruit worden overlegd met de contactpersoon van de business.	NCSC C.07.9
11	Aantoonbaar follow-up geven en verbeteringen doorvoeren dienen te geschieden indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen of verwachtingen, of tekortkomingen opleveren.	NCSC C.07.10
12	Op basis van de geconsolideerde rapportages dienen beveiligingsplannen te worden geactualiseerd en verantwoordelijken toegewezen te worden voor het realiseren van (delen) van het beveiligingsplan.	NCSC C.07.11

Toelichting op maatregelen

01 *Afhankelijk van de typologie van de organisatie is het raadzaam om gelogde gegevens te centraliseren. De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging.*
Er is een plan[3] beschikbaar met daarin activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

02 *Procedurebeschrijving met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.*
Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

04 *In de ontwerp- casu quo configuratie documentatie is vastgelegd waar en hoe correlaties worden aangebracht. Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.*

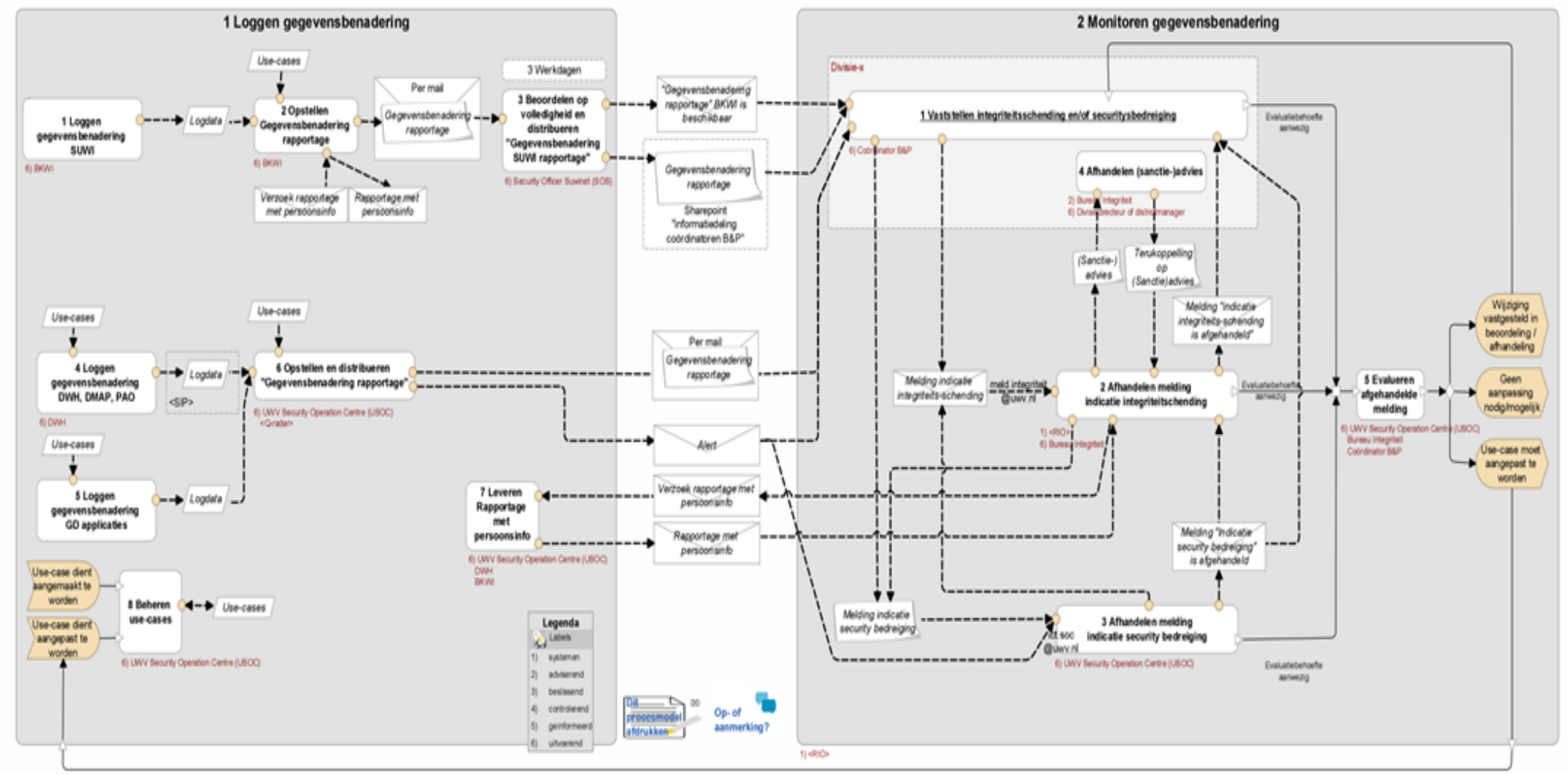
07 *Handmatige acties zijn herleidbaar naar natuurlijke personen.*

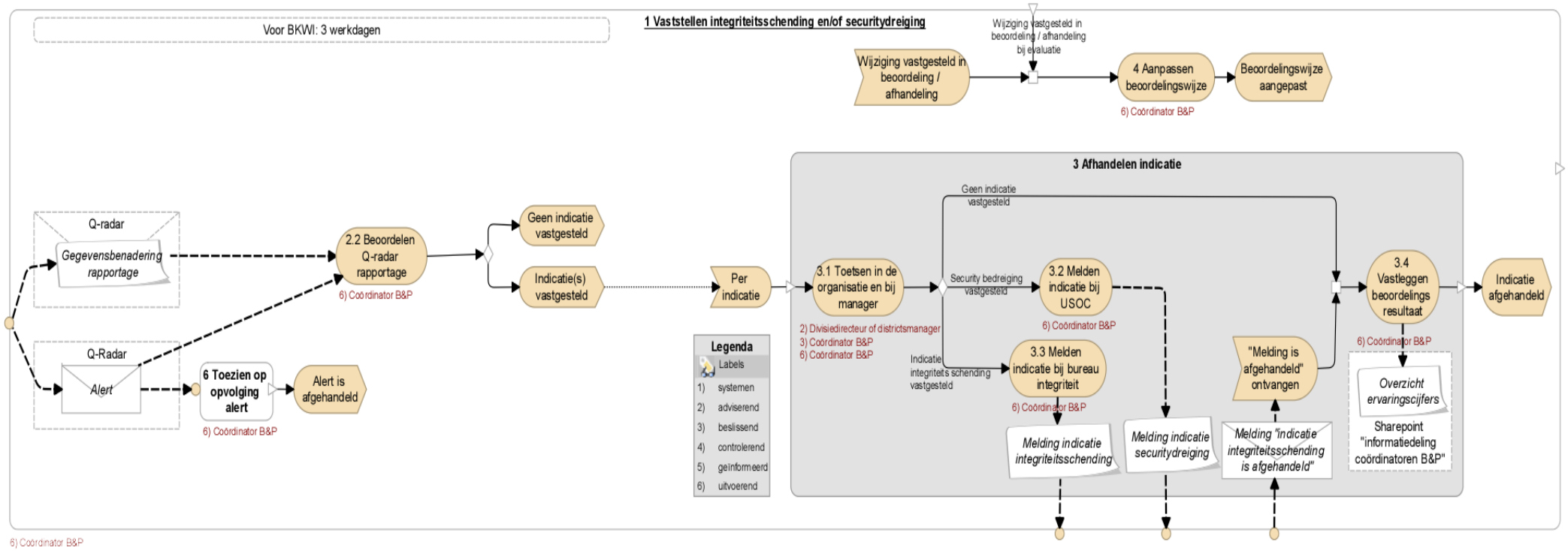
12 *De resultaten uit deze evaluatie worden geconsolideerd en gerapporteerd naar het hoogste management.*

4.3. Monitoringproces applicaties

Op de volgende pagina's treft men een overzichtsplaat aan van het monitoringsproces. Hierbij de link naar het proces waarbij het onderdeel 'vaststellen integriteitsschending op de pagina hierna opengeklapt wordt getoond. Via de link treft met de volledige beschrijving aan. link

[3] Zie proceshuis concern-ict het proces ICT informatiebeveiliging


1 Loggen gegevensbenadering
2 Monitoren gegevensbenadering
1 Loggen gegevensbenadering SUWI
6) BKWI
Logdata
Use-cases
2 Opstellen Gegevensbenadering rapportage
6) BKWI
Verzoek rapportage met persoonsinfo
Rapportage met persoonsinfo
Per mail
Gegevensbenadering rapportage
3 Werkdagen
3 Beoordelen op volledigheid en distribueren "Gegevensbenadering SUWI rapportage"
6) Security Officer Suwinet (SOS)
"Gegevensbenadering rapportage" BKWI is beschikbaar
Gegevensbenadering rapportage
Sharepoint "Informatiedeling coördinatoren B&P"
Divisie-x
1 Vaststellen integriteitsschending en/of securitysbedreiging
6) Coördinator B&P
4 Afhandelen (sanctie-)advies
2) Bureau Integriteit
6) Divisiedirecteur of districtmanager
(Sanctie-) advies
Terugkoppeling op (Sanctie)advies
Melding "indicatie integriteits-schending is afgehandeld"
Evaluatiebehoefte aanwezig
Use-cases
4 Loggen gegevensbenadering DWH, DMAP, PAO
6) DWH
Logdata
<SIP>
Use-cases
6 Opstellen en distribueren "Gegevensbenadering rapportage"
6) UWV Security Operation Centre (USOC)
<Qradar>
Per mail
Gegevensbenadering rapportage
Alert
Use-cases
5 Loggen gegevensbenadering GD applicaties
Logdata
7 Leveren Rapportage met persoonsinfo
6) UWV Security Operation Centre (USOC)
DWH
BKWI
Verzoek rapportage met persoonsinfo
Rapportage met persoonsinfo
Melding indicatie integriteits-schending
meld integriteit @uwv.nl
2 Afhandelen melding indicatie integriteitschending
1) <RIO>
6) Bureau Integriteit
Evaluatiebehoefte aanwezig
5 Evalueren afgehandelde melding
6) UWV Security Operation Centre (USOC)
Bureau Integriteit
Coördinator B&P
Wijziging vastgesteld in beoordeling / afhandeling
Geen aanpassing nodig/mogelijk
Use-case moet aangepast te worden
Use-case dient aangemaakt te worden
Use-case dient aangepast te worden
8 Beheren use-cases
Use-cases
6) UWV Security Operation Centre (USOC)
Legenda
Labels
1) systemen
2) adviserend
3) beslissend
4) controlerend
5) geinformeerd
6) uitvoerend
Dit procesmodel afdrukken
Op- of aanmerking?
Melding indicatie security bedreiging
3 Afhandelen melding indicatie security bedreiging
@uwv.nl
6) UWV Security Operation Centre (USOC)
Melding "indicatie security bedreiging" is afgehandeld
Evaluatiebehoefte aanwezig
1) <RIO>


Voor BKWI: 3 werkdagen
1 Vaststellen integriteitsschending en/of securitydreiging
Wijziging vastgesteld in beoordeling / afhandeling bij evaluatie
Wijziging vastgesteld in beoordeling / afhandeling
4 Aanpassen beoordelingswijze
6) Coördinator B&P
Beoordelingswijze aangepast
3 Afhandelen indicatie
Geen indicatie vastgesteld
Q-radar
Gegevensbenadering rapportage
2.2 Beoordelen Q-radar rapportage
6) Coördinator B&P
Geen indicatie vastgesteld
Indicatie(s) vastgesteld
Per indicatie
3.1 Toetsen in de organisatie en bij manager
2) Divisiedirecteur of districtsmanager
3) Coördinator B&P
6) Coördinator B&P
Security bedreiging vastgesteld
3.2 Melden indicatie bij USOC
6) Coördinator B&P
Indicatie integriteits schending vastgesteld
3.3 Melden indicatie bij bureau integriteit
6) Coördinator B&P
Melding indicatie integriteitsschending
Melding indicatie securitydreiging
"Melding is afgehandeld" ontvangen
Melding "indicatie integriteitsschending is afgehandeld"
3.4 Vastleggen beoordelings resultaat
6) Coördinator B&P
Overzicht ervaringscijfers
Sharepoint "informatiedeling coördinatoren B&P"
Indicatie afgehandeld
Q-Radar
Alert
6 Toezien op opvolging alert
6) Coördinator B&P
Alert is afgehandeld
Legenda
Labels
1) systemen
2) adviserend
3) beslissend
4) controlerend
5) geinformeerd
6) uitvoerend
6) Coördinator B&P

5. SIEM

5.1. Inleiding

Het UWV Security Operations Center (USOC) maakt voor de monitoring van de servers in het HRC gebruik van een SIEM oplossing. Deze verzamelt log gegevens van diverse systemen[4] zowel op operating systeem-, middleware- als applicatie niveau. De SIEM-oplossing ondersteunt het USOC en de business bij het detecteren van mogelijke beveiligingsincidenten en het inzicht verkrijgen in de UWV infrastructuur en helpt het UWV aan de interne en externe regelgeving te voldoen. Op deze wijze kan UWV eventuele afwijkende patronen in samenwerking met de leverancier snel herkennen en hier onderzoek naar doen.

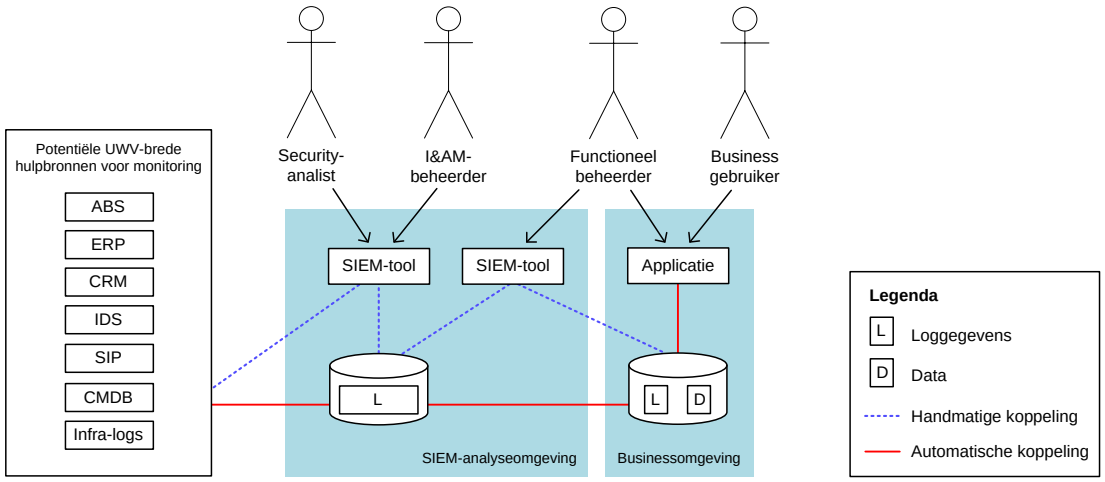
Binnen de Kantoor Automatiseringsomgeving / Werkplek- en Netwerkdiensten (KWN) wordt gemonitord via verschillende op zichzelf staande tooling. Bijvoorbeeld het Anti-Virus dashboard, de internet proxy logging, IDS/IPS, Web Applicatie Firewall logging etc.

Business, geadviseerd door BZ, USOC en CISO hebben in overleg, op basis van risicoanalyses het belang van systemen in het primaire proces en de vertrouwelijkheid van de gegevens in deze systemen vastgesteld (=UWV RAL).

Daarnaast worden in de Architectuur Board(AB+) Project Start Architectuur (PSA) documenten door de Enterprise Security Architect beoordeeld waarbij geëist kan worden dat de nieuwe of gewijzigde applicatie aansluit op het SIEM.

Tenslotte kan het zo zijn dat een applicatie-eigenaar zelf, voor hem of haar moverende redenen, wenst aan te sluiten op de SIEM-oplossing.

Figuur 1 is een schematische weergave van de manier waarop SIEM-tooling qua importeren van logbronnen is opgebouwd.



Figuur 2. Logbronnen en omgevingen

5.2. Criteria en maatregelen voor SIEM oplossingen

Dit hoofdstuk geeft een samenvatting van de beveiligingscriteria (principes of hoofdnormen) en maatregelen voor SIEM.

Voor de criteria en maatregelen geldt dat:

- De criteria randvoorwaarden zijn waaraan moet worden voldaan. Indien niet wordt voldaan aan gestelde criteria moet de afwijking worden toegelicht conform het *Comply or Explain* principe;
- De genoemde maatregelen Best Practice maatregelen zijn die invulling te geven aan het bovenliggende criterium;

[4] Voor details wordt verwezen naar het document "LOMO aansluitproces SOC".

- De criteria en maatregelen aansluiten bij de UWV RAL criteria en de andere genoemde regelgeving uit paragraaf 1.1.

In deze paragraaf zijn de criteria nader toegelicht en voorzien van maatregelen.

LM05 – SIEM		
Criterium (wie en wat)	In netwerken en (web)applicaties zijn signaleringsfuncties effectief en efficiënt ingericht die logberichten genereren, samenvatten en de beheerorganisatie alarmeren.	BIR 10.10.1 NCSC C.06
Doelstelling (waarom)	Het maakt het mogelijk direct op als ernstig gedefinieerde schendingen van functionele en beveiligingseisen te kunnen reageren door snelle alarmering van de beheerorganisatie.	
Risico	Tekortkomingen en zwakheden in de geleverde producten/diensten kunnen niet snel gesignaleerd worden en herstel acties kunnen niet tijdig worden genomen.	

Maatregelen

effectief en efficiënt		
01	In de (web) applicatie-infrastructuur dienen detectiesystemen actief te zijn voor het detecteren van aanvallen.	NCSC C.06.2 SSD-30/01.03
02	In de ontwerp- of configuratie documentatie dient vastgelegd te zijn waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen).	NCSC C.06.3
samenvatten		
03	Systemen die logberichten genereren dienen aangesloten te zijn op een SIEM waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.	BIR 10.10.1.4
alarmeringen		
04	De signaleringssystemen (detectie) dienen tijdig melding van ongewenste gebeurtenissen te maken.	NCSC C.07.2

Toelichting op maatregelen

01 *In de ontwerp- of configuratie documentatie is vastgelegd waar en hoe IDSen worden ingezet. Dit is gebaseerd op een risicoanalyse[5]. De zakelijke behoeften, overwegingen en maatregelen. Rapportage van de risicoanalyse waarop de beslissing is gebaseerd.*

02 *De inrichting is gebaseerd op een vastgesteld inrichtingsdocument / ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging.*
Er is een proces met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, of wanneer geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

03 *Hoewel logs bij voorkeur zo ontworpen worden dat ze voldoende informatie bevatten om te monitoren, is het noodzakelijk afzonderlijke logs te correleren (koppelen) om een goed beeld te krijgen. Dit kan als de voorziening goede filter-, aggregatie- en prioriteringsmogelijkheden biedt.*

04 *In de ontwerp- of configuratie documentatie is vastgelegd welke drempelwaarden gelden voor alarmeringen. Bij alarmeringen gaat het om automatische rapportages gegenereerd door het systeem.*

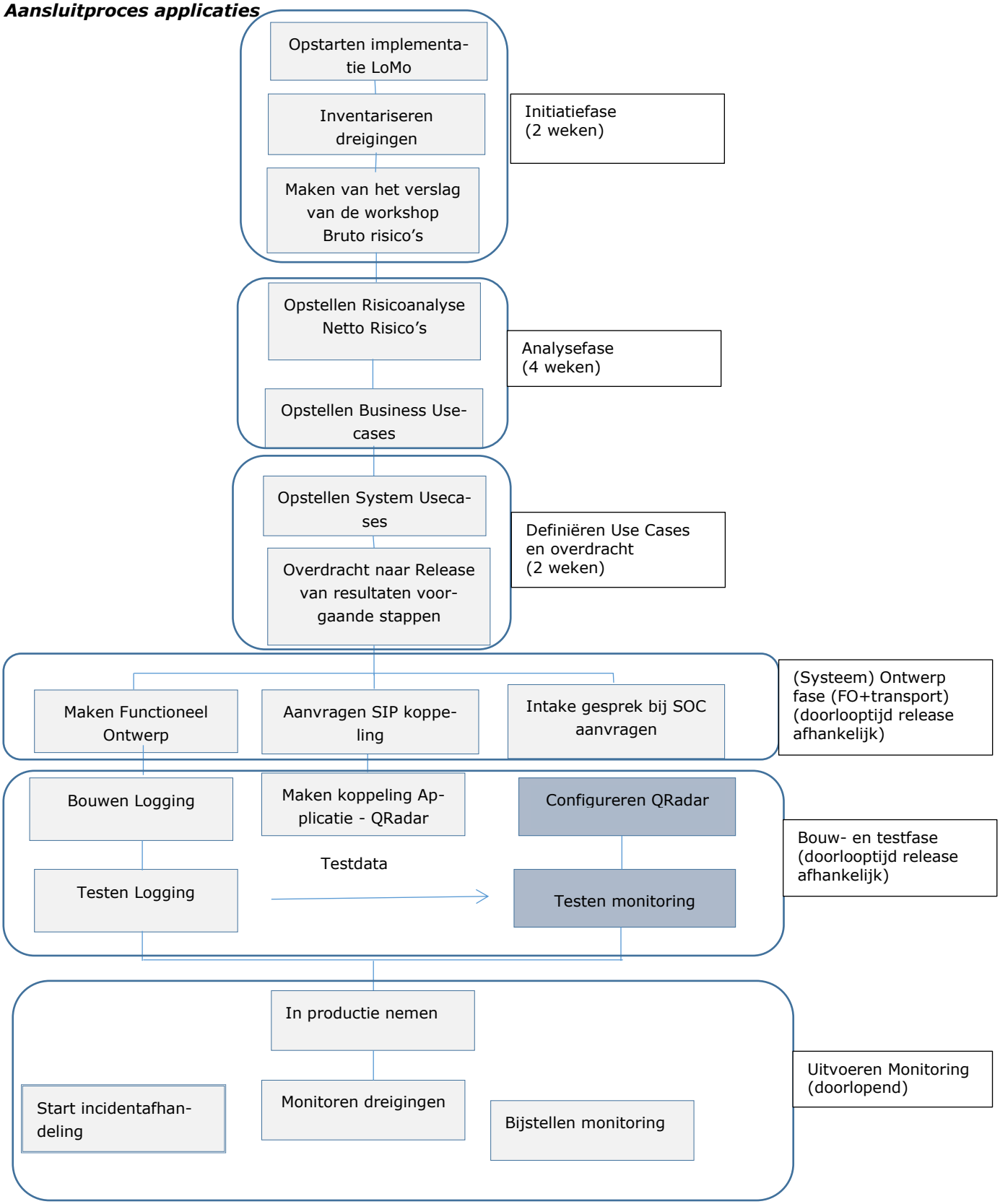
[5] UWV heeft gekozen voor Business IB&P Requirements Analyse (BIRA) als methode voor risicoanalyse.

6. Realisatieproces

6.1. Inleiding

De afgelopen jaren heeft UWV ervaring opgedaan met het aansluiten van IT middelen op het SIEM. Met name bij applicaties waarin gevoelige gegevens zijn opgenomen, heeft dit tot een Best Practice geleid. Daarnaast is ook een uniform monitorproces ontwikkeld waarbij de rollen op basis van bestaande TVB zijn ingevuld. In dit hoofdstuk wordt hier uitleg aan gegeven.

6.2. Aansluitproces applicaties



Bijlage A - Conformiteitsindicatoren

In deze bijlage zijn de relevante conformiteitsindicatoren opgenomen en beschreven, zodat geen onduidelijkheid bestaat over de 'lading' van de indicatoren.

Alarmering
Alarmeringen zijn automatische mededelingen door het detectie systeem voor een naderend gevaar of ongewenste situatie.

Benoemde gebeurtenissen
De te loggen gebeurtenissen die in wet- en regelgeving zijn benoemd.

Beveiligd
Beveiligde inrichting is gerelateerd aan maatregelen met betrekking tot juiste en tijdige werking en beschikbaarheid van de registratie - en detectiefunctie, beveiliging van logbestanden tegen manipulaties, alternatieve paden bij uitval en het veilig stellen van logging bestanden.

Bewaakt
Het (controleren) waarnemen en analyseren (proactief beheren) van informatie ten aanzien van vastgelegde acties in het systeem (trendanalyse). Hierbij worden ook meetwaarden ten opzichte norm/planwaarden bewaakt die zijn bedoeld om uitzonderingen te signaleren (alarmeringen).

Bewaard
De beschikbaarheid van loginformatie waarborgen binnen de bewaartermijn die noodzakelijk wordt geacht en die in de configuratie instellingen van een systeem tot uiting komt.

Effectief en efficiënt
In het webapplicatie domein worden vaak verschillende loggingsmechanismen (registraties) naast elkaar gebruikt. Om de loggingsinformatie niet omslachtig maar met beperkte inspanning en doeltreffend te kunnen analyseren, is van belang deze informatie te centraliseren.

Geanalyseerd
Ontleden en onderzoeken van de vastgelegde loggingsgegevens op bedreigingen en/of ongeoorloofde activiteiten.

Gemonitord
Het bewaken/controleren van (web)applicties en netwerken met als doel ongeautoriseerde toegangspogingen tot systeem - en netwerk resources en ongeautoriseerd gebruik van deze resources tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen.

Gerapporteerd
Het verschaffen van informatie door middel van een uitgebracht verslag over de geanalyseerde logbestanden.

Inbreuk en verstoring
Het ongeautoriseerd aanpassen of manipuleren van logmechanismen/bestanden of (automatisch) overschrijven of verwijderen daarvan.

Minimale set gegevens
De set van gegevens die in overeenstemming met wet- en regelgeving minimaal moet worden vastgelegd in een regel in het logbestand.

Onbevoegde toegang

Het raadplegen, wijzigen, verplaatsen of verwijderen van logbestanden door personen zonder autorisatie daartoe.

Periodiek beoordeeld
Op een vastgestelde periodieke termijn (minimaal eens per maand) beoordelen van log rapportages.

Registratie
Registratie van menselijke- en systeemgerichte acties en van informatie over gebeurtenissen voor controle en analyse doeleinden.

Samenvatten
De functie van detectiesystemen die uit de log bestanden op basis van drempelwaarden meldingen en alarmoproepen voor de beheerorganisatie genereert.

Bijlage B - Toelichting beschrijving normen en maatregelen in SIVA-syntax

Per norm (hierna criterium) wordt in de SIVA methodiek kort aangegeven wat de onderbouwing voor de norm is, met een voorstel voor de te implementeren maatregelen. Bij de beschrijving wordt gebruik gemaakt van het SIVA-raamwerk. Dit bevat vier componenten:

- **S**tructuur;
- **I**nhoud;
- **V**orm;
- **A**nalyse.

De opbouw per beveiligingseis is in de SIVA-syntax, namelijk:

Context
Een beschrijving van het mechanisme.

Na de contextbeschrijving volgt de template voor het beschrijven van een hoofdnorm en de onderliggende sub normen.

Criterium X De Naam van het criterium.		
Criterium	De norm, namelijk '**wie**' en '**wat**'. Het criterium is gelijk aan de norm / architectuurprincipe.	Referenties andere normenkaders
	Wie xxxxx Wat xxxx trefwoord xxx	
Doelstelling	Het gewenste resultaat, namelijk '**waarom**'.	
Risico	Een beschrijving van mogelijk misbruik of schade.	

Maatregelen (of indicatoren)

Trefwoord: Maatregelenreferentie (of Indicatorreferentie)		
Maatregelnr.	De mogelijke maatregelen, namelijk het '**hoe**'. De maatregelen of indicatoren zijn de principle driven rules waaraan invulling wordt gegeven om te voldoen aan het criterium.	Referenties andere normenkaders

Bij de referenties wordt, voor zover relevant, aangegeven waar in de volgende standaarden en richtlijnen additionele informatie is te vinden, zoals:

- UWV BIR, 'Baseline Informatiebeveiliging Rijksdienst', Versie 1.0, 8 december 2014. De UWV BIR is gelijk aan de Rijksbrede BIR van 1 december 2012 met uitzondering van enkele (R)-maatregelen die specifiek op de Rijksdienst zijn gericht. Daar waar deze niet aansluiten bij de UWV-situatie zijn deze aangepast naar de situatie van UWV;

Bijlage C – Bronnen en Afkortingenlijst

De volgende literatuur is geraadpleegd voor het opstellen van Richtlijn Logging en Monitoring.

Titel – interne UWV bronnen	Versie	Datum
Richtlijn Classificatie voor Vertrouwelijkheid	0.94 (1.0?)	22-06-2015
Borging van de BIR beheersing	1.0	08-12-2014
SSD Beveiligingseisen voor webapplicaties	2.0	05-10-2014
QRadar aansluitproces	0.99	11-06-2014
UWV Logging en Monitoringvoor Informatiebeveiliging	3.0	25-10-2012

Titel – externe bronnen	Versie	Datum
NSCS Beveiligingsrichtlijnen web applicaties	0.95	2014
AP Richtsnoeren beveiliging persoonsgegevens	1.0	Februari 2013
AV 21 Goed werken in netwerken AP	2.0	April 2002
NIST SP 800-92 guide to computer security log management	1.0	September 2006
Wet Bescherming persoonsgegevens AP (vervallen per 25-05-2018)	1.0	06-07-2000
Algemene Verordening Persoonsgegevens (AVG) handhaafbaar m.i.v. 25 05 2018	1.0	April 2016
UWV bron opnemen: De risicoclusters zijn vertaald naar een set aan vragen/indicatoren, waaraan vervolgens een wegingsfactor is toege-kend.		
UWV bron opnemen: Selectielijst (zie intranetpagina DIV), die ver-plicht is op grond van artikel 5 van de Archiefwet 1995.		
UWV Bron: Generiek QRadar koppelvlak		

Tabel 2 Referentie documentatie

De volgende literatuur is geraadpleegd voor het opstellen van Richtlijn Logging en Monitoring.

BIR	Baseline Informatiebeveiliging Rijksdienst
BIRA	Business IB&P Requirements Analyse
AP	Autoriteit Persoonsgegevens
CISO	Chief Information Security Officer
HRC	Hoofd Reken Centrum
IDS	Intrusion Detection Systeem
IPS	Intrusion Prevention Systeem
KWN	Kantoorautomatisering, Werkplekdiensten en Netwerkdiensten
LOMO	Logging en Monitoring
NCSC	Nationaal Cyber Security Center
USOC	UWV Security Operation Center
SSD	Secure Software Design
SIEM	Security Information Event System

Tabel 3 Afkortingenlijst

Bijlage D – Te hanteren sjablonen

Zie: https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/IBenP/Technische%20maatregelen/LOMO/Forms/AllItems.aspx