TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Logging

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Aanwijzing logging’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een handreiking voor het gebruik van logging door organisaties binnen de Rijksoverheid.

Doelgroep

Dit document is van belang voor de directie, systeemeigenaren en applicatiebeheerders.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 10.10 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid

Inhoudsopgave

1. Inleiding

De Baseline Informatiebeveiliging Rijksdienst (BIR) beschrijft in hoofdstuk 10.10 maatregelen die te maken hebben met logging, het vastleggen van systeemgebeurtenissen en acties van gebruikers.

Logging is het verzamelen en beoordelen van systeem data en waarschuwingen van bijvoorbeeld applicaties, netwerk infrastructuur, servers en PC's. De eisen die gesteld worden aan logging worden zwaarder naarmate het belang hoger wordt. Loggen is soms noodzakelijk om te kunnen voldoen aan een wettelijke eis, om bijvoorbeeld een audit op een systeem te doen.

1.2 Aanwijzing voor gebruik

Deze handleiding is geschreven om informatiebeveiligingsmaatregelen met betrekking tot logging en controle uit te werken en daarbij handreikingen te geven voor het logging-beleid en logging-procedures. Deze handleiding biedt geen volledige procesbeschrijving ten aanzien van logging.

Dit document gaat daarbij uit van de minimale eisen aan logging op basis van de BIR.

1.3 Leeswijzer

In hoofdstuk 2 wordt een algemene uitleg van logging en een handreiking ten aanzien van logging beschreven. Hoofdstuk 3 gaat in op loggingbeleid voor overheidsorganisaties. In bijlage 1 wordt voorbeeld beleid voor logging geformuleerd en bijlage 2 biedt een handreiking voor communicatie over logging naar medewerkers.

2 Logging

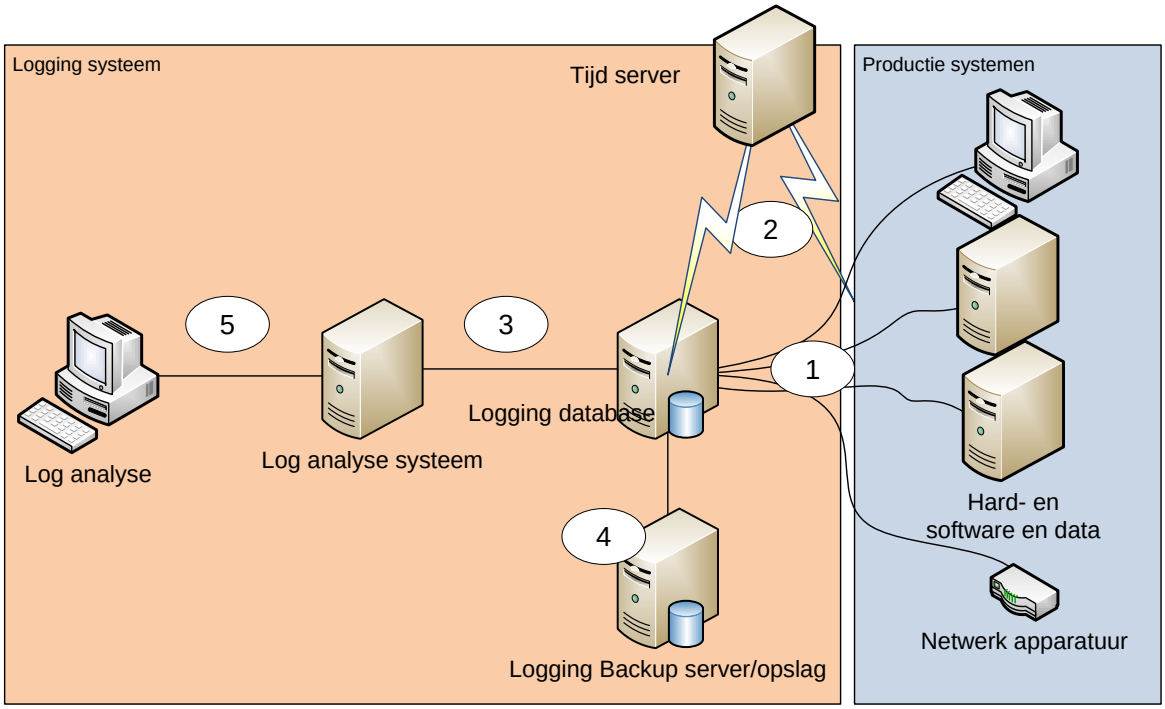
2.1 Inleiding

Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten. In sommige gevallen zijn dit normale statusmeldingen, in andere gevallen is de loginformatie het resultaat van een activiteit van een gebruiker of beheerder of het resultaat van onvoorziene omstandigheden of fouten in systemen. Een log beschrijft wat er gebeurt binnen systemen.

Veel computersystemen gebruiken logging om informatie op te slaan over foutsituaties en andere gebeurtenissen die aandacht behoeven van de gebruiker of beheerder. Een log kan geschreven worden in tekstbestanden maar ook in databasetabellen. Tegenwoordig kunnen de beschrijvingen van systemen zo gedetailleerd zijn dat ze zelfs beschrijven waarom een gebeurtenis heeft plaatsgevonden.

Hoe ziet een log opzet er globaal uit:

1. Logging wordt vanuit de systemen naar een centrale logging database gezonden.
2. Alle systemen hebben dezelfde tijd en gebruiken een tijd synchronisatie bron.
3. De logging database wordt benaderd vanuit een loganalyse systeem.
4. Logging die langere tijd ongebruikt blijft, wordt apart gezet in een back-up server.
5. Het loganalyse systeem wordt gebruikt door loganalyse werkstations.



Een logging systeem dient gescheiden te zijn van andere systemen. Er dient alleen toegang te zijn voor de medewerkers die logging moeten beoordelen of voor auditors.

2.2 Logging soorten

In de BIR worden de volgende vormen van logging onderkend:

- Automatische logging, zoals Technische Logging en Audit Logging;
- Handmatige logging, zoals logboeken van beheerders over uitgevoerde werkzaamheden, zoals het starten van een back-up of het wisselen van de back-up tapes.

Automatische logging

Automatische logging wordt door systemen en netwerken zelf verzorgd. Voor de automatische logging dienen instellingen op de verschillende systemen te worden geactiveerd. Naast de normale systeemlogging, die betrekking heeft op bepaalde activiteiten van alle gebruikers, dienen de activiteiten van beheerders op uitgebreidere wijze gelogd te worden (bijvoorbeeld het gebruik van speciale en hoge privileges op het systeem). Bij het bepalen van instellingen wordt het gestelde beleid voor beveiliging en controle op logging als uitgangspunt genomen. De ingestelde logging dient de performance van de systemen niet negatief te beïnvloeden.

Technische logging (ook wel controle van systeemgebruik genoemd) is het vaststellen of informatiesystemen correct worden gebruikt, goed worden beheerd en functioneren conform de gestelde eisen is uit bijvoorbeeld een SLA. In de technische logging dienen gebeurtenissen te worden opgenomen, zoals het gebruik van technische- en functionele beheerfuncties, handelingen van beveiligingsbeheer, verstoringen in het productieproces en beveiligingsincidenten. Voorbeelden van beveiligingsincidenten zijn: de aanwezigheid van malware, resultaten van het testen op zwakheden of vulnerabilities, foutieve inlogpogingen, 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: het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur en het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen.

Audit logging, in de zin van de BIR, is het vastleggen van activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole (zie ook “bewaartermijnen”).

Verschillen tussen technische en audit logging

Wat	**Technische log**	**Audit log**
Voor wie	Operator, ontwikkelaar, auditor	Security, auditor
Logging conditie	Niet voor alle systemen aan	Altijd aan
Inhoud van de logging	Fouten, handelingen,	Aanvallen, activiteiten,

	uitvoeren van functies	fouten
Scope	Niet altijd bekend	Van te voren bekend
Tijdsduur	Zinvol voor uren tot dagen	Afhankelijk van classificatie, jaren

Handmatige logging

Naast de automatische systeemlogging zijn beheerders zelf verantwoordelijk voor het bijhouden van een handmatig geregistreerd logboek, al dan niet in opgeslagen in digitale vorm. In dit logboek worden alle belangrijke beheerwerkzaamheden opgenomen. Hierbij dient te worden opgemerkt dat het niet de bedoeling is dat beheerders van minuut tot minuut een vastlegging van werkzaamheden moeten opstellen. Als stelregel kan worden gebruikt dat alle grote en kritische beheerswerkzaamheden en ook alle werkzaamheden en situaties die afwijken van de dagelijkse activiteiten worden vastgelegd in het logboek. De beheerder vermeldt hiertoe in het logboek de datum en het tijdstip van uitvoering, de reden van de uitvoering, een omschrijving van de uitgevoerde werkzaamheden en het resultaat van deze werkzaamheden.

2.3 Loggen over logging en controle

Ook over logging dient weer gelogd te worden om achteraf aan te tonen dat een logbestand niet is gewijzigd of dat iemand toegang heeft gehad:

- Het openen van een nieuw logbestand, maar ook het verwijderen ervan dient te worden gelogd.

Ook beheerders mogen logbestanden niet wijzigen en als dit toch gebeurt, dient dit ook weer gelogd te worden. Dit kan op een apart systeem beter worden ingeregeld.

Voer actief controles uit op logs

Het is belangrijk dat een organisatie actief controles uitvoert op de verzamelde logs. Alleen op die manier kan een organisatie misbruik van de omgeving en inbraakpogingen detecteren. Er moeten daarom procedures worden opgesteld waarin staat beschreven hoe en wanneer controles op logs moeten plaatsvinden en hoe taken op dit gebied belegd zijn. De verantwoordelijke moet in zijn taak ondersteund worden door een deugdelijke filtering op de logs. Alleen bij een deugdelijke filtering is het mogelijk om aanvallen te detecteren uit de grote hoeveelheid informatie binnen de logs die de verschillende componenten op een dag zullen genereren. Filtering van de logs zal bij voorkeur dynamisch zijn. Door het filter continu aan te passen ontstaat een behapbaar en bruikbaar overzicht van gebeurtenissen die zich in de omgeving hebben voorgedaan.

2.4 Logging-cyclus en -opslag

Het maken van een log dient in een cyclus te gebeuren anders worden de logbestanden of logtabellen in een database te groot. Het is doorgaans niet nodig om door middel van logs ver in de tijd terug te kunnen kijken. De bewaartermijn is afhankelijk van het belang van de log.

In systemen kan worden bepaald hoe vaak een logbestand moet worden vernieuwd. Dit kan bijvoorbeeld bij het bereiken van een bepaalde loggrootte of op een bepaald moment. Bij het bereiken van die grens start een nieuw logbestand en het oude logbestand wordt bewaard. Het is raadzaam om goed na te denken over de rotatie van de log en de bewaarlocatie van de logbestanden. De omvang van logbestanden kunnen namelijk de prestaties van systemen degraderen en ruimte innemen die noodzakelijk is voor de werking van systemen. Meestal worden logbestanden op een andere plaats (centraal) neergezet. Het apart opslaan van logbestand heeft een aantal voordelen:

1. De grootte van een logbestand op een productiesysteem is in de hand te houden.
2. Logbestanden kunnen makkelijker beveiligd worden tegen onbevoegd wijzigen. Separate opslag kan apart worden beveiligd.
3. De bewaartermijn van een log kan beter worden nageleefd. Een log moet soms gedurende een minimum termijn bewaard worden, maar er zijn ook maximum termijnen (veelal in relatie tot privacy).

2.5 Waar te loggen?

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

1. SYSLOG
   SYSLOG is een standaard voor computerlogging. De logging is gescheiden tussen systemen die de logging genereren en systemen die de logging opslaan.
2. SNMP
   SNMP staat voor Simple Network Management Protocol. Dit protocol kan worden gebruikt voor het besturen van netwerkapparaten. Het protocol voorziet ook in statusmeldingen (traps).
3. Windows Event log
   De Windows Event log is standaard in de Windows-besturingssystemen aanwezig en kan ook naar een centrale logvoorziening worden verzonden.
4. Losse logbestanden
   Hier kan het gaan om tekstbestanden, kommagescheiden (CSV)-bestanden en andere varianten die lastig te monitoren zijn. Deze bestanden moeten voor gebruik in een centrale logomgeving worden geanalyseerd en vertaald door de logvoorziening.
5. Database logging, applicatie logging
   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. Vaak gaat het hier om audit logging.
6. Logging van beveiligingssystemen, zoals Intrusion Detection Systems

Beveiligingssystemen genereren logs die bij voorkeur naar een centraal systeem worden verzonden. Dit omdat bij een geslaagde aanval ook de logging gecompromitteerd kan raken en een aanvaller zal trachten zijn sporen uit te wissen door hierbij te komen.

Al deze verschillende mechanismen voor logging zorgen ervoor dat de logging versnipperd raakt. De organisatie kan hierdoor het overzicht over alle gebeurtenissen gemakkelijk kwijt raken. Om bijvoorbeeld aanvallen efficiënt te kunnen detecteren, is het van belang alle logs op één centraal punt bijeen te brengen. Hoewel een organisatie er in de praktijk niet aan ontkomt om verschillende mechanismen voor logging in te zetten, is het altijd aan te raden om de diversiteit hierin zoveel mogelijk te beperken. Door de logs op een centraal punt bijeen te brengen en filtering toe te passen op deze logs, ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur. Dit kan het format hebben van een platte tekst maar het kan ook een database zijn. 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.

2.6 Meerwaarde van logging

Een juiste wijze van logging kan veel waardevolle informatie opleveren voor uiteenlopende zaken als beheer, onderhoud, rapportages en informatiebeveiliging. Logging kan gebruikt worden voor het:

- ondersteunen van capaciteitsbeheer door het krijgen van statusinformatie van systemen;
- ondersteunen bij het ontdekken van fouten in soft- en hardware;
- ontdekken van menselijke fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen;
- ontdekken van corruptie van data of programmatuur en antivirusmeldingen;
- ondersteunen bij forensisch onderzoek van systemen;
- ondersteunen van onderzoek na een incident;
- implementeren van Security Incident en Event Management systemen (SIEM);
- ondersteunen van SLA Compliance Monitoring;
- leveren van informatie ten behoeve van een wettelijk voorgeschreven audit;

- leveren van informatie om te onderzoeken of voldaan wordt aan beleid (bijvoorbeeld of er vreemde apparaten aangesloten zijn geweest);
- leveren van informatie om onweerlegbaar aan te tonen dat een bepaald bericht wel of niet verzonden is, of dat een activiteit is uitgevoerd;
- rapporteren over systeemgebruik en incidenten aan de systeemeigenaar en de Chief Information Security Officer (CISO).

Het is wenselijk om een juiste logging aanpak te ontwikkelen. Hierbij wordt de volgende volgorde voorgesteld: (1) log zoveel mogelijk informatie, (2) bewaar datgene dat nodig is, (3) analyseer regelmatig en (4) rapporteer op basis van de analyse.

2.7 Belangrijke knelpunten bij logging

Door de potentiële waardevolle informatie die logging kan opleveren, is het zaak om de belangrijkste knelpunten voor logging te onderkennen. Deze zijn:

1. Niet standaard loggen
   Veel systemen loggen niet standaard. Logging dient veelal als optie aangezet en geconfigureerd te worden. Een technische logging op systeem niveau werkt bijvoorbeeld vaak nog wel, echter de audittrail logging van de webserver die draait, is niet standaard geactiveerd.
2. Niet kijken naar logging.
   Als er wordt gelogd, dan wordt deze logging niet altijd regelmatig of op tijd bekeken, terwijl dit volgens wet- en regelgeving noodzakelijk kan zijn of uit een risicoanalyse kan blijken dat logging en het regelmatig bekijken ervan noodzakelijk is.
3. Te weinig loggen of te kort/te lang bewaren.
   Het te kort bewaren van de informatie in een log of te weinig informatie loggen, omdat ruimte beperkt is, is een belangrijk knelpunt om goed gebruik te kunnen maken van loggen. Bij een incident is het vervolgens niet mogelijk ver genoeg terug in de tijd te kunnen kijken. Soms worden logs juist te lang bewaard. Dit kost onnodig ruimte.
4. Verkeerde logging prioriteit.
   Er wordt veelal besloten alleen bepaalde informatie in een log op te slaan. Bij een incident wordt vervolgens pas vastgesteld dat er informatie mist in de log.
5. Geen logging van applicaties
   Er zijn vele soorten applicaties, van legacy systemen tot moderne systemen, die mogelijk functionaliteit voor loggen hebben. Voor ieder kritiek systeem dienen logregels (beleid) te bestaan en te worden nageleefd.
6. Beperken tot bekende fouten.
   Vaak wordt gezocht naar een bekende fout met een loganalyse-tool, terwijl er vaak meer te ontdekken is door er met een andere bril (andere loganalyse-software of andere parameters) naar te kijken.
7. Verkeerde aannames ten aanzien van loggen.
   De relatie tussen een event en een transactie van een gebruiker is niet altijd eenduidig vast te leggen. In veel gevallen levert een transactie een veelvoud aan log events op, die niet altijd herleidbaar zijn tot een transactie.

2.8 Bewaartermijnen van een log

Hieronder worden de bewaartermijnen inclusief het standaard niveau van de BIR ('hoog' voor Integriteit, 'vertrouwelijk' voor vertrouwelijkheid) beschreven. De bewaartermijnen van een log worden nader beschreven in het operationele product bij de BIR voor dataclassificatie.

Integriteit

Niveau	Monitoring
Niet zeker	Geen
Beschermd	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoringgegevens bewaren voor periode van een half jaar.
Hoog	**Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoringgegevens bewaren voor periode van maximaal twee jaar of langer bij een vermoed beveiligingsincident.**
Absoluut	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoringgegevens bewaren voor periode van minimaal drie jaar bij een vermeend beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.

Vertrouwelijkheid

Niveau	Monitoring
Openbaar	Geen
Bedrijfs- vertrouwelijk	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van een half jaar.
Vertrouwelijk	**Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van twee jaar.**
Geheim	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van zeven jaar.

In de BIR staat ook beschreven wat de relevante input en output van een ICT-systeem of -service is, dat vastgelegd dient te worden in een log. Deze relevante input en output is:

- een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
- de gebeurtenis (zie BIR 10.10.2.1);
- waar mogelijk de identiteit van het werkstation of de locatie;
- het object waarop de handeling werd uitgevoerd;
- het resultaat van de handeling;
- de datum en het tijdstip van de gebeurtenis.

De volgende gebeurtenissen dienen gelogd te worden:

- gebruik van technische beheerfuncties;

- gebruik van functionele beheerfuncties;
- handelingen van beveiligingsbeheer;
- beveiligingsincidenten;
- verstoringen in het productieproces;
- handelingen van gebruikers;
- online transacties.

2.9 Logging en SaaS

Software-as-a-Service (SaaS) wordt steeds vaker gebruikt om informatie te verwerken. Ten aanzien van logging is het probleem bij SaaS is, dat de informatie binnen de systemen van de leverancier van de SaaS-oplossing in de databases is verwerkt. Bij de aanbieder van de SaaS zal antwoord op de volgende vragen gekregen moeten worden:

- Welke logs (kunnen) worden gemaakt?
- Welke garanties krijgt bestaan er dat logs niet gewijzigd zijn?
- Welke afspraken worden aangegaan opdat logs indien nodig dagelijks worden beoordeeld?
- Welke rapportages kunnen verwacht worden omtrent logging?
- Kunnen logs automatisch naar worden verzonden?
- Welke garanties biedt de SaaS-provider?
- In welk formaat zijn de logs?
- Zijn de gegevens binnen de log leesbaar, of te importeren in een beschikbaar logplatform?

2.10 Wat te doen bij uitvallen van de logging

Het inzetten van logging brengt een belangrijk vraagstuk met zich mee: wat te doen op het moment dat de logging uitvalt? Dit kan gelden voor de centrale logging maar ook voor de decentrale logging.

Als er niet meer gelogd kan worden, bestaat de kans dat niet meer kan worden aangetoond wie toegang heeft gehad tot een systeem of tot gegevens. Ook bestaat de kans dat niet meer vastgesteld kan worden 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 zijn te maken:

1. De component normaal te laten functioneren en geen logging opslaan.
   De component normaal laten functioneren terwijl deze de logs niet kan opslaan.
   Consequentie hiervan is dat de logs verloren gaan

2. De component lokaal te laten loggen en later de logging te synchroniseren.
   Veel componenten beschikken over een eigen mechanisme om lokaal te loggen. Daarmee kan de log tijdelijk worden veiliggesteld. Op het moment dat het centrale logmechanisme weer beschikbaar komt, sluist de component de verzamelde logs alsnog door. Dit voorkomt dat de component uit productie genomen moet worden en voorkomt tevens dat logs verloren gaan. Er moet wel voor gewaakt worden dat de

lokale logging er niet tot gevolg heeft dat alle beschikbare ruimte van het systeem verbruikt wordt. Op het moment dat de lokale opslag volloopt, moet opnieuw besloten worden wat de component hierna doet (in productie blijven – zie bovenstaande optie - of uit productie halen – zie volgende optie).

3. De component uit productie te nemen
   De component acuut uit productie halen. Dit betekent dat gebruikers niet meer kunnen werken met het systeem. Stoppen met verwerking betekent dat compromitteren niet meer ongemerkt kan plaatsvinden en ook dat de audit log geen hiaten gaat vertonen. Er zijn maar enkele systemen die zo belangrijk zijn dat deze vorm van ingrijpen nodig is.

2.11 Communicatie over logging

Het is aan te bevelen om over logging transparant te zijn tegenover eindgebruikers van systemen. Hiervoor kan een paragraaf worden toegevoegd aan de arbeidsovereenkomst. Daarnaast staat in bijlage 2 een voorbeeld van mogelijke communicatie over logging naar eindgebruikers.

3 Logging-controle

3.1 Inleiding

Het is belangrijk dat een organisatie actief controles uitvoert op verzamelde logs. Alleen op die manier kan een organisatie misbruik van de omgeving en inbraakpogingen detecteren. Er moeten daarom procedures zijn opgesteld waarin staat beschreven hoe en wanneer controles op logs moeten plaatsvinden en hoe taken op dit gebied zijn belegd.

De verantwoordelijke moet daarbij in zijn taak ondersteund worden door een goede automatische filtering op de logs. Alleen bij een goede filtering is het mogelijk om aanvallen te detecteren uit de grote hoeveelheid informatie binnen de logs die de verschillende componenten op een dag genereren. Filtering van de logs zal bij voorkeur dynamisch zijn. Door het filter continu aan te passen ontstaat een behapbaar en bruikbaar overzicht van gebeurtenissen die zich in de omgeving hebben voorgedaan.

Controle van de logs kan met speciale software gedaan worden. In een eerste fase kan ook gestart worden met handmatige controle van logs. Dit levert direct inzicht op en voeding voor een geautomatiseerd controle in een volgende fase.

3.2 Eerste logging stappen voor baseline

Als er nog niet actief gelogd wordt binnen de infrastructuur van de organisatie, is het belangrijk om de logging stap voor stap uit te breiden naar alle hard- en software componenten. Loggen en de controle hierop kost menskracht, tijd en geld. Het is daarom beter om klein te beginnen en dit op termijn uit te breiden naar uiteindelijk een volledig geautomatiseerde logging en logging management-oplossing of naar een Security Information and Event Management (SIEM)-oplossing. Het alleen handmatig beoordelen van alle logs is ondoenlijk. Bij voorkeur dient geautomatiseerd begonnen te worden.

Om vanuit een situatie waarin nog niet wordt gelogd te gaan voldoen aan de verplichtingen uit de baseline, kan het volgende groeipad gekozen worden:

1. Begin met de wettelijk vereiste systemen die gelogd moeten worden.
2. Begin met de ’perimeter’, de buitenkant van het netwerk van de organisatie en de systemen en netwerk componenten in de zogenaamde Demilitarized Zone (DMZ).
3. Vervolgens de netwerkcomponenten binnen het netwerk van de organisatie.
4. De essentiële systemen, applicaties, databases, servers et cetera.
5. De belangrijke systemen, applicaties, databases, servers et cetera.
6. Alle overige systemen.

De volgende stappen kunnen doorlopen worden om per onderdeel uit het groeipad met loggen te beginnen:

1. Bepaal het systeem waarvan de logging gecontroleerd dient te worden.
2. Haal uit de BIR welke informatie gelogd moet worden.
3. Bepaal waar de opslag van de logs moet plaats vinden, per systeem en centraal.
4. Zorg voor gelijk afgestelde systeemklokken.
5. Bepaal wie de logging dagelijks naloopt als taak, per systeem en wijs die taak toe.

6. Richt een proces in om de logs na te lopen en te rapporteren, bepaal een Log Baseline.
7. Schoon de logs regelmatig op, volgens de BIR na twee jaar, en bewaar de incidenten.
8. Rapporteer over het beoordelen van de logs aan de systeemeigenaren en de CISO.

3.3 Overige aandachtspunten bij logging

Herleidbaarheid

Zoals in hoofdstuk 3.1 wordt ingegaan op het proces en de documentatie van logging, is daarnaast ook de herleidbaarheid van een logregel naar een event belangrijk. Van een gecollecteerde log regel, of log regel rapportage moet een 'chain of custody' aantoonbaar zijn. Dit heeft betrekking op een specifiek systeem, een specifiek timeframe, een specifieke gebruiker, en het is compleet, en niet veranderd. Om dit door middel van een handmatig logging proces goed op orde te krijgen, is erg veel werk. Herleidbaarheid is alleen mogelijk door een goede log infrastructuur aan te leggen en gebruik te maken van technologieën zoals: caching, encryptie, hashing, en gecontroleerde toegang tot de opslag van de logging.

Timestamp management

Naast het gelijk laten lopen van systeemklokken, is het belangrijk om per logregel aandacht te hebben voor timestamping. Het gaat hier om het vastleggen van de tijdstippen die in het logproces zelf ontstaan, zoals:

- tijd van generatie van het log event;
- tijd van ontvangst door het centrale log systeem;
- tijd van beoordeling.

Originerend systeem

Het systeem dat de logregel veroorzaakt, staat vaak niet in de logregel zelf. Als dat het geval is, dient het logsysteem deze toe te voegen aan de opgenomen logregel.

Herkenning en parsing[1]

Rapportages en filters worden pas zinvol en deterministisch als logregels goed herkend en geparsed worden. Een gefaalde login moet als dusdanig gemarkeerd worden, met de parameters die van belang zijn. Indien dit mechanisme ontbreekt, blijft de rapportage het resultaat van een toevallige zoekactie naar aanwezigheid van bepaalde tekst.

[1] Een parser (van het Engelse to parse, ontleden, en het Latijnse pars, deel) is een computerprogramma, of component van een programma, dat de grammaticale structuur van een invoer volgens een vastgelegde grammatica ontleedt (parset). Een parser zet ingevoerde tekst om in een datastructuur. Vergelijk het met het invullen van een formulier met gegevens op de voorgegeven plaats in een voorgegeven tekstformaat, zoals bloktekst (wikipedia).

Beschikbaarheid en toegankelijkheid

Een incident meldt zichzelf niet als dusdanig in de logs, bijvoorbeeld: als je 'A' ziet dan is er echt iets aan de hand. Een incident wordt zichtbaar door één of meedere logregels die opvallen. Het herkennen van een incident kan derhalve alleen als *alle* relevante logs snel en makkelijk beschikbaar, toegankelijk en zoekbaar zijn. Dit proces kan (deels) geautomatiseerd worden met een SIEM-oplossing, waarbij in een duidelijke context sneller het verschil tussen incidenten en niet-incidenten te geven is.

Retentie

Binnen het loggingsysteem dient gegarandeerd te worden dat logevents bewaart worden voor een bepaalde termijn, maar ook niet langer dan dat. Na afloop van de termijn, is de logregel niet meer beschikbaar.

3.4 Controle op logs: een voorbeeld proces

Om een indruk te geven van de hoeveelheid stappen die doorlopen kunnen worden bij het controleren van logregels, is hieronder een voorbeeld van een controleproces globaal uitgewerkt als best practice. Het bevat alle onderdelen die benodigd kunnen zijn bij het beoordelen van logregels. Dit proces kan handmatig doorlopen worden, maar ook gebruikt worden voor inrichting van de workflow binnen tooling die wordt ingezet voor het controleren van logregels.

Eén van de basisstappen die doorlopen kan worden, is het 'baselinen' van logregels. Bij baselinen worden bekende logregels gedocumenteerd per systeem of applicatie. Deze baseline kan dan bij de periodieke controle van de log worden gebruikt om vast te stellen of een logregel 'normaal' is of niet.

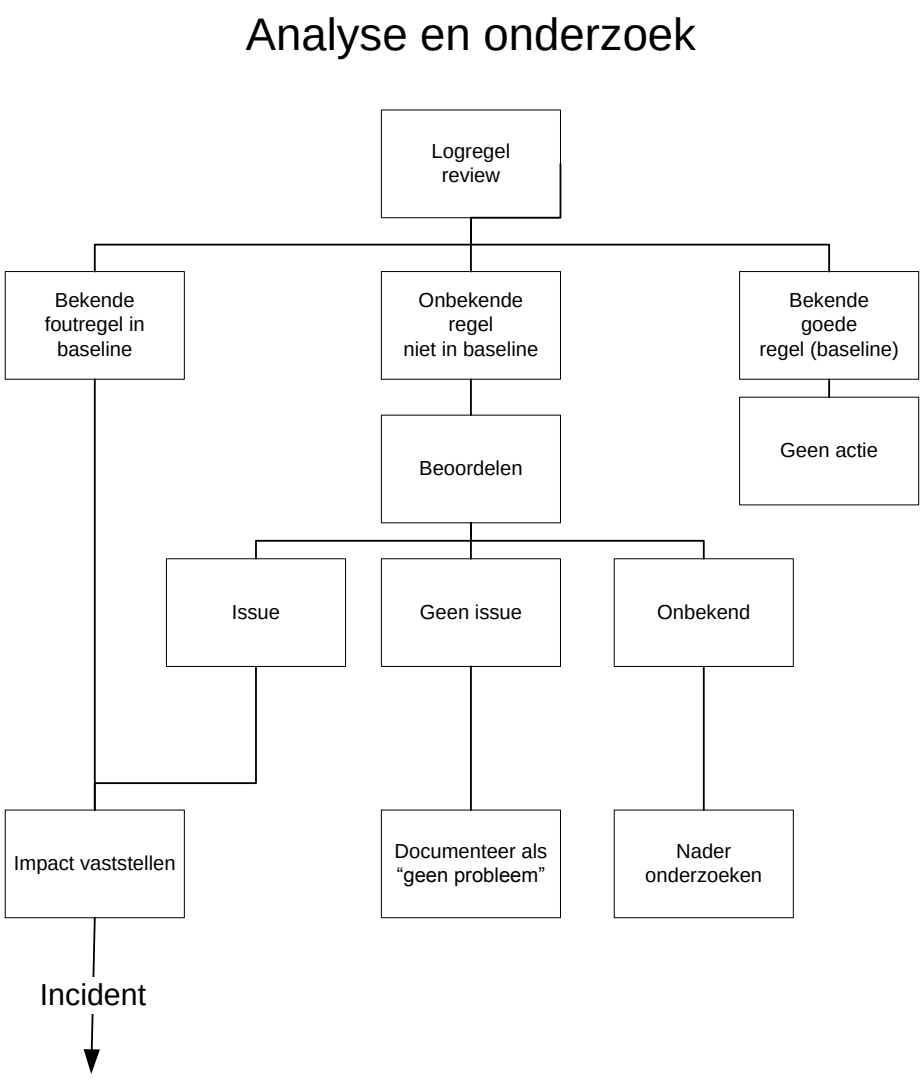
Stappen die doorlopen kunnen worden om logs te baselinen:

1. Zorg ervoor dat de logs op één plaats zijn opgeslagen.
2. Selecteer een periode voor de initiële Log Baseline, bijvoorbeeld 90 dagen.
3. Doorloop de log van de oudste naar de jongste regel.
4. Maak een samenvatting van de gevonden soorten logregels.
5. Als er geen incidenten gevonden zijn, dan is deze samenvatting de baseline van 'normale' logregels. Als er toch verdachte of bekende fouten gevonden worden dienen deze als 'bekende fouten' ook in de logbaseline te worden opgenomen. Voorbeelden van deze fouten zijn:
   a. Inloggen en rechten toekennen op ongebruikelijke tijdstippen
   b. Toegangsrechten die veranderen buiten het venster voor wijzigingen
   c. Logberichten van oude user accounts
   d. Reboot/opstartberichten buiten een Service Window
   e. Verwijdering van loggegevens
   f. Back-up/export van data buiten back-up vensters
   g. Het stoppen van logging van een systeem of applicatie
   h. Alle overige logregels die mogelijk geassocieerd kunnen worden met overtredingen van het beveiligingsbeleid

Dagelijkse controle van logs

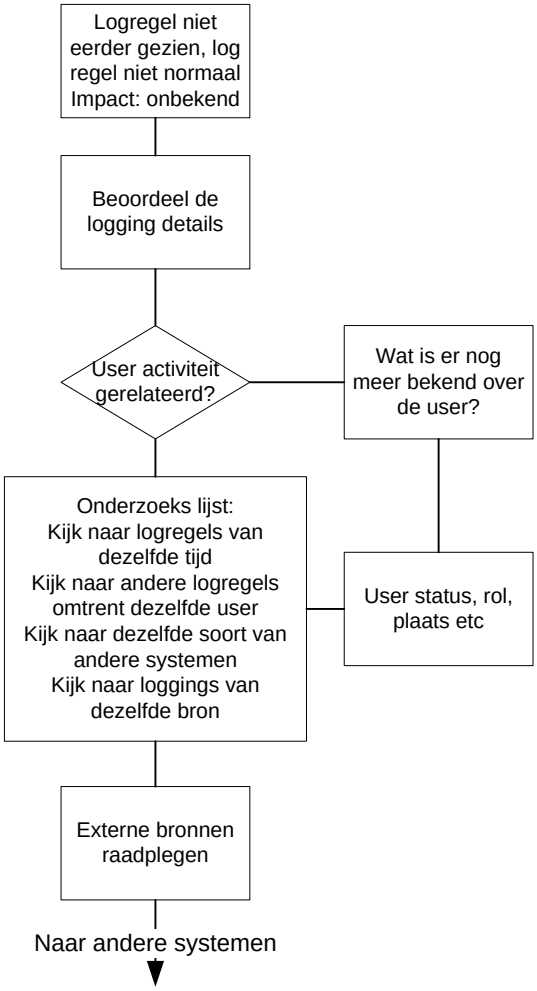
Na het opbouwen van de baseline kan gestart worden met de (dagelijkse) controle activiteiten op de logs. De eerste stap bij het beoordelen van een log is het uitvoeren van analyse en onderzoek. Bij deze analyse worden logregels vergeleken met de logbaseline. In dit proces worden bekende foutregels in de baseline na het bepalen van de impact gekwalificeerd als een 'incident'. Bekende goede regels worden genegeerd. Onbekende logregels worden beoordeeld waarbij er drie keuzes zijn:

- Issue – van deze logregel wordt de impact vastgesteld en een incident aangemeld en deze wordt aan de logbaseline toegevoegd als bekende foutregel.
- Geen issue – deze logregel wordt aan de baseline toegevoegd als bekende goede regel.
- Onbekend – deze logregel wordt in de volgende stappen verder beoordeeld.



Voor onbekende logregels dient het volgende proces te worden gevolgd. De logregel die niet normaal is en waarvan de impact onbekend is, wordt eerst verder beoordeeld. Er moet worden vastgesteld of de logregel gerelateerd is aan een gebruiker van het systeem: is deze gebruiker bekend, wat zijn de rechten? Tevens dient te worden gezocht in andere logs rond hetzelfde tijdstip als dat nodig is. Documenteer alle gevonden gegevens voor verder onderzoek.

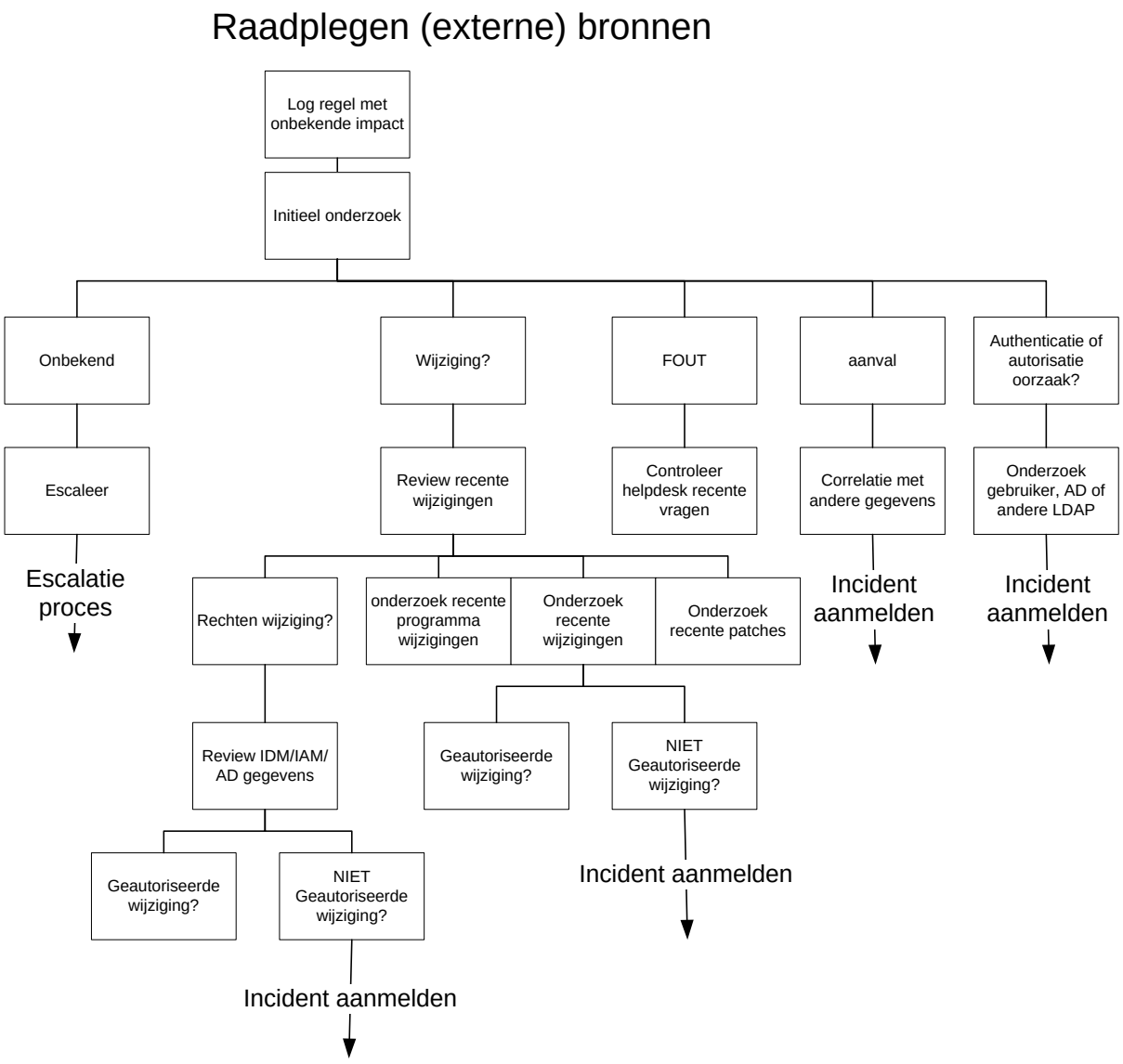
Logregel initieel onderzoek en user onderzoek



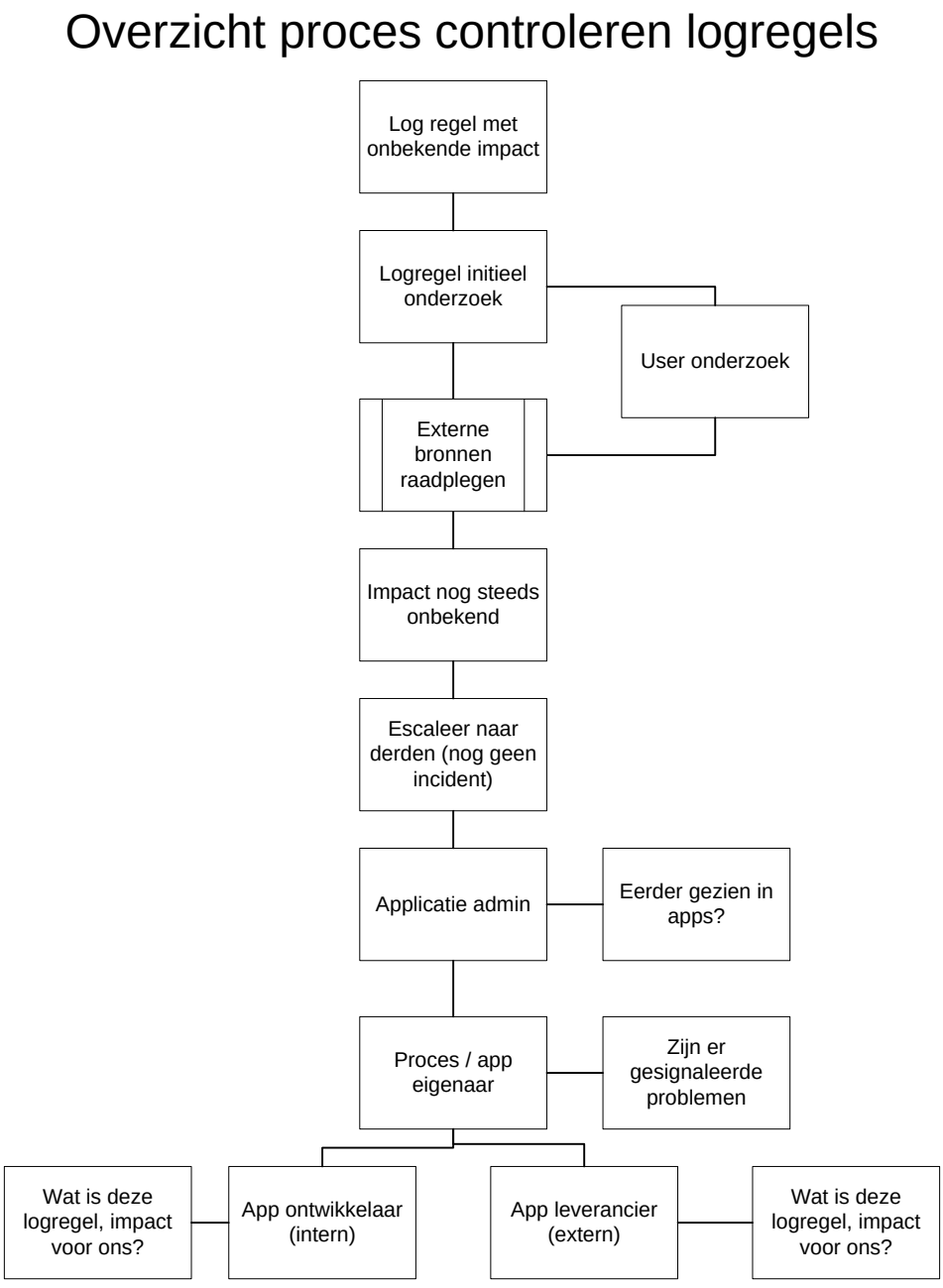
De volgende stap voor het identificeren van logregels is het raadplegen van externe bronnen. Het doel van deze procedure is het identificeren van informatiebronnen waar verder gezocht kan worden, gebaseerd op het type logregel en vervolgens om het effect en de vereiste acties (indien aanwezig) te identificeren. De procedure start met de identificatie van

de aard van de vermelding in de logregel en daarbij worden vervolgens de relevante informatiebronnen geraadpleegd.

Indien er niets gevonden kan worden in een externe bron dient naar derden te worden geëscaleerd, daarmee wordt hier bedoeld dat er ‘derden’ nodig kunnen zijn voor het beoordelen van de logregel. Het belangrijkste idee van de stap ’escaleer naar derden’ is om de juiste mensen die kennis zouden kunnen hebben te vinden en vervolgens te interviewen. De laatste stap is het raadplegen van de ontwikkelaar van de applicatie geraadpleegd of dat de leverancier van de toepassing een support vraag wordt gesteld. Dit hangt af van support contracten en beantwoording van deze vragen kan geld en tijd kosten.



Hier wordt het totale proces weergegeven waarbij ook de voorgaande stappen vereenvoudigd worden weergegeven.



3.5 Bewijsvoering

Een belangrijk onderdeel van onderzoek (ook review genoemd) aan een log is het zorg dragen dat er voldoende bewijs is van het gevolgde proces, de implementatie van de gevolgde stappen en het gevonden resultaat. Dit is noodzakelijk als logging-issues moeten dienen als onderdeel van de bewijsvoering in (bv. arbeidsrechtelijk of strafrechtelijk)

onderzoek. De processtappen voor de bewijsvoering komen overeen met de stappen die nodig zijn voor de rapportage aan het management over de logging en log review-processen.

De volgende documentatie is nog voor een juiste bewijsvoering door middel van logs:

1. Het hebben van en het toereikend zijn van de logging.

Deze sectie is de makkelijkste van de drie om te bewijzen. De volgende items dienen als bewijs van de logging:

   a. Gedocumenteerd loggingbeleid, dat zowel ingaat op het registreren van gebeurtenissen als de gelogde details.
   b. Beschrijving van de configuratie van systeem- en applicatielogging op basis van het loggingbeleid.
   c. De geproduceerde loggingbestanden van de applicaties op basis van het beleid.

2. Het hebben van log review-processen en de implementatie ervan.

Dit gedeelte is moeilijker te bewijzen ten opzichte van de vorige. De volgende items dienen als bewijs van log beoordeling:

   a. Gedocumenteerd loggingbeleid, dat ook de beoordeling van de log voorschrijft.
   b. Gedocumenteerde operationele procedures, waarin de exacte stappen zijn beschreven voor het beoordelen van de logs.
   c. Logboeken van logbeoordelingstaken die zijn uitgevoerd (dit kan soms ook door tooling worden verzorgd).
   d. Verslagen van het onderzoeken van uitzonderingen kunnen dienen als indirect bewijs dat de beoordeling van de log heeft plaatsgevonden (zie ook volgende paragraaf).

3. Exception Handling Proces en de uitvoering ervan.

Dit gedeelte is verreweg het moeilijkst te bewijzen. De volgende items dienen als bewijs van log review van de uitzonderingen (exceptions):

   1. Gedocumenteerd loggingbeleid, waarin het onderzoek van uitzonderingen (exceptions) en hun behandeling zijn gedocumenteerd.
   2. Gedocumenteerde operationele procedures, waarin de exacte stappen die ondernomen worden om afwijkingen te beoordelen die gevonden zijn tijdens de logcontrole.
   3. Een logging van alle onderzochte uitzonderingen (exceptions) en welke acties zijn uitgevoerd.

Logbeoordeling logboek

Het logboekbewijs van onderzoeksuitzonderingen (Exception of Investigations), waarin de uitzonderingen tijdens de dagelijkse beoordeling zijn gemarkeerd, wordt onder meer gebruikt als bewijs van naleving van loggingbeleid. In het logboek moeten alle betrokken systemen zijn opgenomen, alle mensen die zijn geïnterviewd, alle acties en hun motiveringen, tot welk resultaat het heeft geleid, welke tools en commando's er werden gebruikt (met welke resultaten), et cetera. Het volgende hoofdstuk beschrijft de inhoud van de registratie in het logboek.

Een registratie in het logboek moet het volgende bevatten:

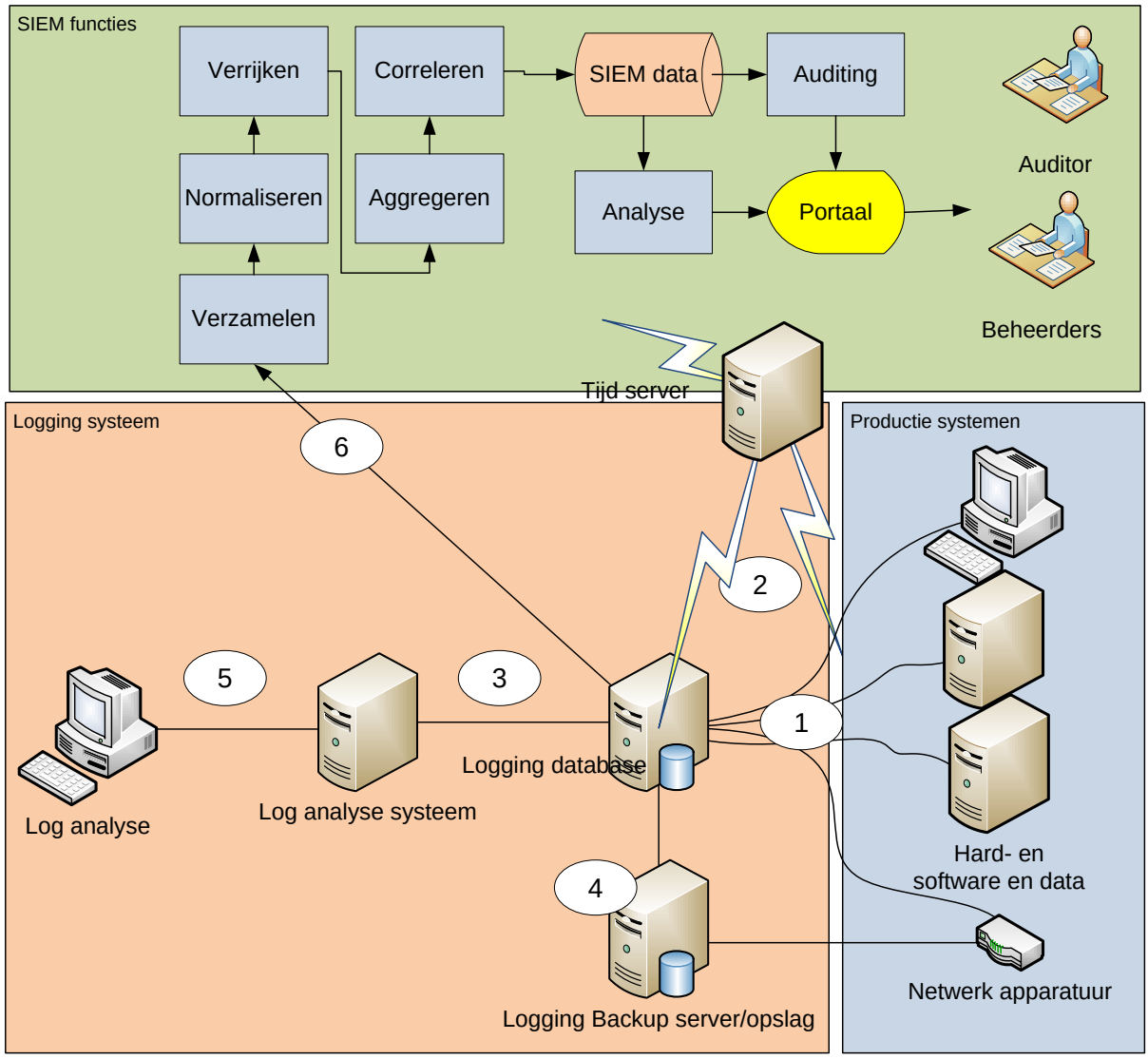
1. Datum/tijd/tijdzone waarop de registratie in het logboek werd gestart.
2. Naam en functie van de persoon betreffende de registratie in het logboek.
3. Waarom wordt gestart: loguitzondering (gekopieerd uit de logaggregatie tool of uit het oorspronkelijke logbestand), ervoor zorgen dat de gehele log wordt gekopieerd, in het bijzonder de tijdstempel ervan (wat/wanneer/waar, et cetera).
4. Gedetailleerde beschrijving waarom de regel in het logboek niet routine is en waarom deze analyse wordt uitgevoerd.
5. Informatie over het systeem:
   - Host naam
   - Operating System (OS)
   - Naam van de toepassing
   - IP-adres(sen)
   - Locatie(s)
   - Eigenaarschap (indien bekend)
   - Belang van het systeem (indien gedefinieerd en van toepassing)
   - Informatie over Patch Management status, Change Management status, et cetera
6. Informatie over de gebruiker die in de logging gevonden is (indien van toepassing).
7. Gevolgde procedure en gebruikte tools, gemaakte screenshots et cetera.
8. Onderzoek acties die zijn uitgevoerd en uitgezet.
9. Mensen waarmee contact is geweest gedurende het onderzoek.
10. Bepaalde impact gedurende de analyse.
11. Aanbevelingen voor acties en genomen maatregelen (indien nodig).

3.6 Security Information and Event Management (SIEM)

Een Security Information and Event Management (SIEM)-tool is een systeem van voorzieningen, die voorziet in het continu loggen en realtime monitoren van beveiligingsmaatregelen en alerts die worden veroorzaakt door afwijkend gedrag in infrastructuren en applicaties. Het voorziet in lange termijn opslag van verzamelde gegevens en in historische- en trendanalyse van die gegevens. Tevens biedt het functies voor incident alerting en forensisch onderzoek.

Vanuit de bronsystemen word informatie verzameld door het Security Event en Information Monitoring systeem. Een SIEM-systeem voert de volgende bewerkingen uit:

- Verzamelen
- Normaliseren
- Verrijken
- Aggregeren
- Correleren



Het eerdere logging plaatje aangevuld met SIEM-functies.

De implementatie van een SIEM heeft de meeste toegevoegde waarde als er een goede logging basis is, er goede ‘use cases’ zijn, en er dient ook geïnvesteerd te worden in capaciteit om de SIEM te monitoren. Ook een SIEM gaat uit van een vorm van een baseline doordat het een context opbouwt. Er kan realtime worden geanalyseerd tegen de opgebouwde context. De context kan bijvoorbeeld bestaan uit een lijst met ICT-beheerders uit de active directory of een lijst met bekende gebruikers die van buiten de organisatie mogen inloggen.

Bijlage 1: Logging-beleid <organisatie>

Beleidsuitgangspunten Logging <organisatie>

Ten behoeve van de beveiliging van informatie is er een loggingbeleid voor alle ICT-voorzieningen. Het doel van dit beleid is duidelijke regels te beschrijven over logging binnen de organisatie.

De <naam organisatie> hanteert de volgende beleidsuitgangspunten welke zijn ontleend aan de BIR en aanvullend zijn op het algemene beveiligingsbeleid van de organisatie:

Uitgangspunten Audit logging

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

1. Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2. Een logregel bevat minimaal:
   - Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
   - De gebeurtenis (zie BIR 10.10.2.1)
   - Waar mogelijk de identiteit van het werkstation of de locatie:
     - Host naam
     - Operating System (OS)
     - Naam van de toepassing
     - IP-adres(sen)
     - Locatie(s)
     - Het object waarop de handeling werd uitgevoerd
   - Het resultaat van de handeling
   - De datum en het tijdstip van de gebeurtenis
3. In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de organisatie zelf (dus wel gebruikersnamen of inlog accounts).
4. Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM). Hiermee worden (gecorreleerde) meldingen en alarmoproepen aan de beheerorganisatie gegeven. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
5. Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt ook gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld een logserver die niet bereikbaar is).

6. Alle ongeautoriseerde toegangspogingen zijn beveiligingsincidenten en vereisen directe opvolging door melding aan de informatiebeveiligingsfunctionaris.

Controle van het beleid op systeemgebruik

Er zijn procedures vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is, kan ook gebruik gemaakt worden van een logboek door bijvoorbeeld beheerders.

De volgende gebeurtenissen worden in ieder geval opgenomen in de logs:

1. Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instellingen: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
2. Gebruik van functies voor functioneel beheer, zoals het wijzigingen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases).
3. Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord resetten, uitgifte en intrekken van cryptosleutels.
4. Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van Security Services).
5. Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen).
6. Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
7. Online transacties. Hierbij wordt gelogd: het bericht-ID, datum en tijd, aanroepend en verzendend systeem en -proces.

Bescherming van informatie in logbestanden

Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:

1. Logfaciliteiten en informatie in logbestanden dienen te worden beschermd tegen inbreuk en onbevoegde toegang.
2. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
3. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
4. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.

5. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden, zal daarbij altijd het ‘vier ogen’ principe toegepast worden.
6. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
7. Het goed functioneren van de logging wordt continue gemonitord voor essentiële systemen.
8. Controle op opslag van de logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is).

Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van de organisatie behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

1. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.

Aldus vastgesteld door de directie van *[organisatie]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____

Bijlage 2: Communicatie over logging van toegang tot en gebruik van systemen

Logging

De organisatie heeft rapportages ontwikkeld omtrent het vastleggen (logging) van het gebruik van systemen. De organisatie is verplicht om gegevens te loggen waarmee het gebruik van applicaties per medewerker van de organisatie kan worden nagegaan.

De volgende gegevens worden gelogd:

1. Het tijdstip van iedere login en logout en andere acties.
2. De gebruikersnaam van degene die inlogt/uitlogt.
3. Persoonsgegevens (of enige andere zoeksleutel) waarvan gegevens worden opgevraagd. Dit wordt als actie geregistreerd.
4. Elke actie, zoals de bekeken applicatie pagina's, overzichten en mutaties.

Het doel van deze logging is onder andere:

Het tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking van gegevens:

1. Ter ondersteuning van verplichte audits over bepaalde systemen.
2. Wetenschappelijke en/of statistische doeleinden.

De eindgebruikers van systemen moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met systemen:

1. Het bestaan van de logging-applicatie.
2. De (aard van de) gegevens die binnen deze applicatie worden gelogd.
3. Doelen van de logging.
4. Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd.
5. De wijze en het moment waarop en door wie een onrechtmatig of doel overschrijdend gebruik van systemen wordt geconstateerd.
6. Dat bij bovenstaande constatering dit door het afdelingshoofd wordt gecommuniceerd met de betreffende medewerker(s).

In het kader van de beveiliging worden de gegevens over het gebruik van applicaties eens per drie maanden uitgevraagd.

Het betreft dan de volgende gegevens:

1. Inkijkacties
2. Opvragingen persoonsgegevens

3. Geldig ten opzichte van ongeldig rol gebruik
4. Inlogpogingen
5. Administrator accounts
6. Accounts per status
7. Opvragingen per pagina
8. Geregistreerde ten opzichte van actieve accounts.

De logginggegevens worden door de applicatiebeheerder beoordeeld.