INFORMATIE
BEVEILIGINGS
DIENST

AANWIJZING LOGGING

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Aanwijzing Logging

Versienummer
1.0.1

Versiedatum
Juli 2016

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Opmerkingen
1	Januari 2014	
1.0.1	Juli 2016	Taskforce BID verwijderd, WBP vervangen door Wbp, GBA vervangen door BRP en contactgegevens IBD aangepast

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van zo'n project.

Hoe realiseert de IBD haar doelen?
Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de website en community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten.
Onderhavig product is onderdeel van het productenportfolio.
Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: Wbp, BRP, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, , waarbij er in de naleving van dat kader ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Het doel van dit document is een aanwijzing te geven over het gebruik van logging binnen gemeentelijke systemen.

Doelgroep
Dit document is van belang voor het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Informatiebeveiligingsbeleid van de gemeente
- Incident Management en Response Beleid

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
Heel hoofdstuk 10.10.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) heeft maatregelen beschreven die te maken hebben met logging (in casu het vastleggen van) van systeemgebeurtenissen en acties van gebruikers. Zie hiervoor hoofdstuk 6.1 'Controle' in het gemeentelijk informatiebeveiligingsbeleid en hoofdstuk 10.10 van de BIG.

1.1 Doelstelling Aanwijzing Logging

Doelstelling van Aanwijzing Logging is het verzamelen en beoordelen van systeem data en waarschuwingen van bijvoorbeeld applicaties, netwerk infrastructuur, servers en desktop PC's. Goed loggen is soms noodzakelijk om te kunnen voldoen aan een wettelijke eis, om bijvoorbeeld een audit op een systeem te doen. De eisen die gesteld worden aan logging worden zwaarder naarmate het belang hoger wordt. Hiervoor beschrijft het IBD document over dataclassificatie de specifieke eisen. Dit document gaat uit van de minimale eisen aan logging op basis van de BIG.

1.2 De indeling van dit document is als volgt:

Hoofdstuk 1: Inleiding
Hoofdstuk 2: Algemene uitleg en aanwijzingen over logging
Hoofdstuk 3: Logging-beleid
Bijlage: Beleidsuitgangspunten logging
Bijlage: Communicatie over logging naar medewerkers

1.3 Aanwijzing voor gebruik

Deze handleiding is qua opzet 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 is niet een volledige procesbeschrijving.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

2 Logging

Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten.
Een log beschrijft wat er gebeurt binnen systemen. Tegenwoordig zijn de beschrijvingen van systemen soms zo gedetailleerd dat ze beschrijven waarom een gebeurtenis heeft plaatsgevonden.

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.

Goede logging kan gebruikt worden voor:

- Het ondersteunen van capaciteitsbeheer door het krijgen van statusinformatie van systemen.
- Het ondersteunen bij het ontdekken van fouten in soft- en hardware.
- Het ontdekken van menselijke fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen.
- Het ontdekken van corruptie van data of programmatuur en antivirusmeldingen.
- Het ondersteunen bij forensisch onderzoek van systemen.
- Het ondersteunen van onderzoek na een incident.
- Als basis voor implementatie van Security Incident en Event Management systemen (SIEM).
- Het ondersteunen van SLA Compliance Monitoring.
- Het leveren van informatie ten behoeve van een wettelijk voorgeschreven audit;
- Het leveren van informatie om te onderzoeken of voldaan wordt aan beleid (bijvoorbeeld of er vreemde apparaten aangesloten zijn geweest).
- Het leveren van informatie om onweerlegbaar aan te tonen dat een bepaald bericht wel of niet verzonden is, of dat een activiteit is uitgevoerd.
- Rapportage over systeemgebruik en incidenten aan de systeemeigenaar en de Chief Information Security Officer (CISO).

Logging is een van de minst gewaardeerde onderwerpen voor ICT-beheerders omdat ze vaak de middelen of de tijd niet hebben om een log goed te kunnen lezen. Het loggen van veel verschillende informatie in verschillende formaten vanuit verschillende systemen maakt het niet eenvoudig om hier goed mee om te gaan. Daarnaast wordt er vaak te veel of juist te weinig gelogd.

In een log moet het volgende worden weergegeven, de zogenaamde vijf W's:
- Wat gebeurde er?
- Wanneer gebeurde het?
- Waar gebeurde het?
- Wie was betrokken?
- Waar komt het vandaan?

Wat zijn de belangrijkste fouten die gemaakt worden bij logging?

1. Niet loggen: Veel systemen loggen niet standaard, je moet logging als optie aanzetten en configureren, bijvoorbeeld: een technische logging op systeem niveau werkt vaak nog wel, echter de audittrail logging van de webserver die draait, is niet standaard geactiveerd.
2. Niet kijken naar logging, bijvoorbeeld: Als er al wordt gelogd, dan wordt deze logging niet regelmatig bekeken, soms als het te laat is en soms helemaal niet. Terwijl uit wetgeving of uit een risicoanalyse blijkt dat logging en het regelmatig bekijken ervan verplicht is.
3. Te weinig loggen of te kort/te lang bewaren, bijvoorbeeld: te kort bewaren van de informatie in een log of te weinig informatie loggen omdat ruimte beperkt is waardoor het bij een incident niet mogelijk is ver genoeg terug in de tijd kunnen kijken. Of te lang bewaren, bijvoorbeeld omdat men denkt dat een termijn van zeven jaar nodig is terwijl dat niet zo is, dit kost onnodig ruimte.
4. Verkeerde logging prioriteit: bijvoorbeeld er wordt besloten alleen bepaalde informatie in een log op te slaan en bij een incident vaststellen dat er informatie mist in de log. De juiste volgorde is: Log alles, bewaar alles wat nodig is, analyseer en rapporteer met regelmaat een subset van de gegevens.
5. Geen aandacht hebben voor logging van applicaties: Er zijn bijvoorbeeld vele soorten applicaties van legacy systemen tot moderne systemen die allemaal wel/niet loggen. Bovendien hebben ontwikkelaars van systemen vaak geen oog voor logging of er worden daaraan vaak geen eisen gesteld. Voor ieder kritiek systeem dienen logregels (beleid) te bestaan en te worden nageleefd.
6. Kijken naar bekende fouten, bijvoorbeeld; er 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. Foute aannames op basis van loggen, bijvoorbeeld: De relatie tussen een event en een transactie van een gebruiker is niet altijd makkelijk vast te leggen. In veel gevallen levert een transactie een veelvoud aan log events op, die niet altijd herleidbaar zijn tot een transactie.

2.1 Logging-cyclus en -opslag

Het maken van een log dient in een cyclus te gebeuren. Dit omdat anders de logbestanden of -tabellen in een database te groot worden. Het is vaak ook niet direct nodig om erg ver in de tijd terug te kunnen kijken. In systemen kan men soms bepalen hoe vaak een logbestand moet worden vernieuwd, dat kan bijvoorbeeld op loggrootte, op -tijdstip of -datum en dit is tevens systeemafhankelijk. Dus als er een grens overschreden wordt, 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, dit omdat logbestanden door hun omvang ook de prestaties van een systeem kunnen degraderen en ruimte innemen die noodzakelijk is voor de werking van een systeem. Meestal probeert men logbestanden op een andere plaats (centraal) neer te zetten, dit heeft een aantal voordelen:

1. De grootte 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.

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

- 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.

2.2 Logging soorten

In de BIG worden de volgende vormen van logging onderkend:

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

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: 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 in grote mate op een negatieve wijze te beïnvloeden.

Technische logging (BIG – controle van systeemgebruik)
Het doel van de controle van systeemgebruik is vaststellen of informatiesystemen correct worden gebruikt, goed worden beheerd en functioneren conform de gestelde eisen in 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
Volgens de BIG dienen activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. Zie ook “bewaartermijnen”.

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.

Wat zijn de verschillen tussen de twee vormen van loggen

Wat	**Audit log**	**Technische log**
Voor wie	Security, auditor	Operator, ontwikkelaar, auditor
Logging conditie	Altijd aan	Niet voor alle systemen aan
Inhoud van de logging	Aanvallen, activiteiten, fouten	Fouten, handelingen, uitvoeren van functies
Scope	Van te voren bekend	Niet altijd bekend
Tijdsduur	Afhankelijk van classificatie, jaren	Zinvol voor uren tot dagen

2.3 Bewaartermijnen van een log

Bewaartermijnen van een log zijn beschreven in het document "Handreiking Dataclassificatie", onderdeel van de BIG OP, onder de verschillende eisen voor integriteit en vertrouwelijkheid van gegevens. Hieronder een samenvatting van de bewaartermijnen, met in **VET**gedrukt de BIG standaard:

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. Monitoring-gegevens 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. Monitoring-gegevens 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. Monitoring-gegevens 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. Monitoring-gegevens bewaren voor periode van een half jaar.
Vertrouwelijk	**Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van twee jaar.**
Geheim	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van zeven jaar.

In de BIG staat ook wat relevante input en output van een ICT-systeem of -service is, deze relevante input en output is:

- Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
- De gebeurtenis (zie BIG 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

2.4 Waar te loggen?

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

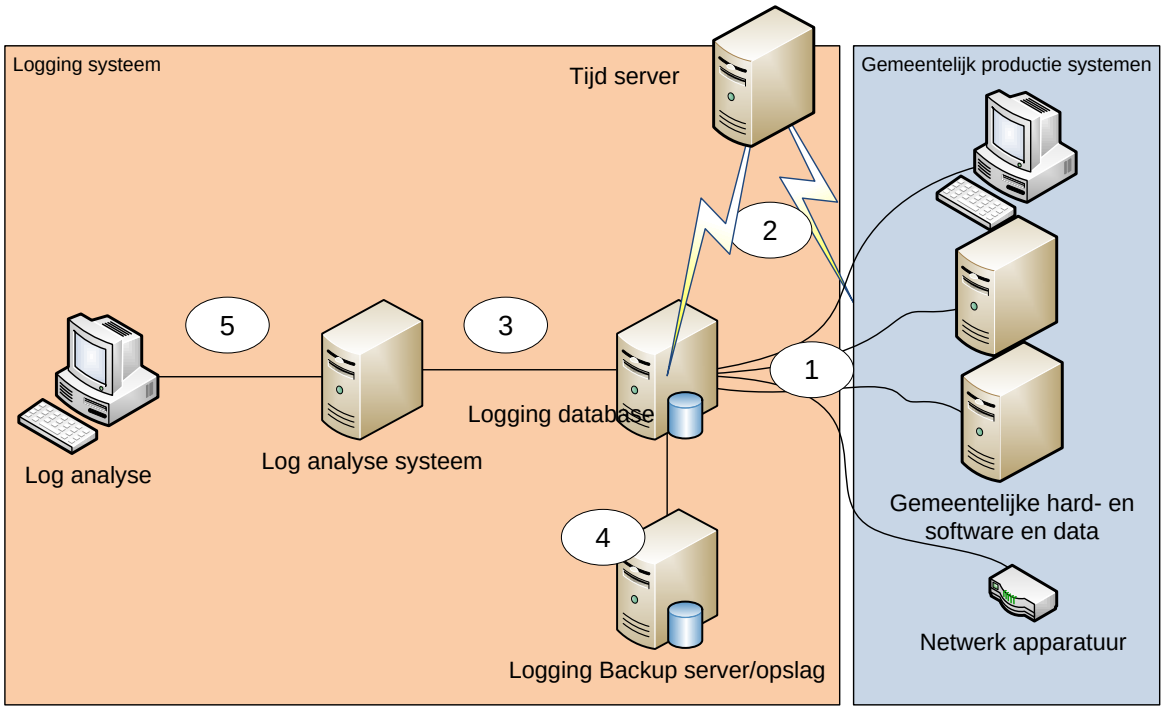
1. SYSLOG
   SYSLOG is een standaard voor computerlogging. De logging is gescheiden tussen systemen die de logging genereren en systemen die de logging opslaan.
2. SNMP
   SNMP staat voor Simple Network Management Protocol. Dit protocol kan worden gebruikt voor het besturen van netwerkapparaten. Het 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
   Dit is de lastigste variant omdat het hier kan gaan om tekstbestanden, komma gescheiden (CSV) bestanden en andere varianten. 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 logs genereren die ook bij voorkeur naar een centraal systeem worden verzonden. Dit omdat bij een geslaagde aanval ook de logging gecompromitteerd raakt en een aanvaller zal trachten zijn sporen uit te wissen door hierbij te komen.

Al deze verschillende mechanismen voor logging zorgen ervoor dat logging versnipperd raakt en een organisatie het overzicht over alle gebeurtenissen gemakkelijk kwijt kan raken. Om bijvoorbeeld aanvallen efficiënt te kunnen detecteren is het van belang deze logs op één centraal punt weer 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 in platte tekst maar ook in 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 geisoleerde incidenten te detecteren, zoals een systeeminbraak die zich in meerdere, verschillende stappen laat herkennen.

Hoe ziet een log opzet er globaal uit:



Het logging systeem is gescheiden van de gemeentelijke systemen. Er is alleen toegang voor de medewerkers die logging moeten beoordelen of voor auditors.

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.

2.5 Logging en SaaS

Software-as-a-Service (SaaS) wordt steeds vaker gebruikt om informatie te verwerken. Het probleem bij SaaS is, dat de informatie binnen de systemen van de leverancier van de SaaS-oplossing in de databases verwerkt is. U zult zich bij SaaS de volgende vragen moeten stellen en daarop antwoorden moeten krijgen:

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

2.6 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 geldt 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.

De volgende keuzes zijn te maken:
1. De component normaal te laten functioneren en geen logging opslaan
2. De component lokaal te laten loggen en later de logging te synchroniseren
3. De component uit productie te nemen

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

2. De component normaal laten functioneren en de logs lokaal laten opslaan. 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 voor zorgt 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 acuut uit productie laten 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, bijvoorbeeld het systeem voor burgerzaken.

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.

2.7 Communicatie over logging

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

3 Logging-controle

Voer actief controles uit op logs
Als er wordt gelogd, maar niemand kijkt ernaar, dan is loggen zinloos om uit te voeren. 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 zijn 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.

Controle van de logs kan met speciale software gedaan worden. Echter om te beginnen kan ook gestart worden met het bepalen welke logs belangrijk zijn en daarna volgens een vast proces deze logs eerst handmatig na te lopen.

Waarmee te beginnen
Als er nog niet actief gelogd wordt binnen de gemeentelijke infrastructuur is het ondoenlijk om direct met logging te beginnen van 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 die ook kan doorgroeien naar een Security Information and Event Management (SIEM) oplossing. Het puur en alleen handmatig beoordelen van alle logs is ondoenlijk, begin bij voorkeur geautomatiseerd.

Als er nog niet gelogd wordt en men wil beginnen om aan de Baseline Logging te voldoen kan men beter een groeipad als volgt beginnen:

1. Begin met de wettelijk vereiste systemen die gelogd moeten worden, BRP/SUWI et cetera.
2. Begin met de ‘perimeter’, de buitenkant van het netwerk van de gemeente en de systemen en netwerk componenten in de Demilitarized Zone (DMZ).
3. Netwerkcomponenten binnen het gemeentelijke netwerk.
4. De essentiële systemen, applicaties, databases, servers et cetera.
5. De belangrijke systemen, applicaties, databases, servers et cetera.
6. De overige systemen.

Welke stappen kunnen doorlopen worden om met loggen te beginnen:

1. Bepaal het systeem waar men de logging van wil controleren.
2. Haal uit de BIG 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 BIG na twee jaar, en bewaar de incidenten.
8. Rapporteer over het beoordelen van de logs aan de systeemeigenaren en de CISO.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

3.1 Waar nog meer op te letten bij loggen

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, zo niet onmogelijk. Herleidbaarheid is alleen mogelijk door een goede log infrastructuur aan te leggen en gebruik te maken van technologieën zoals: caching, enryptie, hashing, en gecontroleerde toegang tot de opslag van de logging.

Timestamp management
Los van het gelijk laten lopen van systeemklokken is het belangrijk om bij logging 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

En dit per logregel.

Originerend systeem
Het systeem dat de logregel veroorzaakt staat vaak niet in de logregel zelf, in dat geval moet het logsysteem deze toevoegen 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.

Beschikbaarheid en toegankelijkheid
Een incident meldt zichzelf niet als dusdanig in de logs, bijvoorbeeld: als je 'A' ziet dan is er echt iets 'B' aan de hand. Een incident ontstaat door één of meedere logregels die opvallen. Dit resulteert in nader onderzoek en is als conclusie wellicht een incident. Dit werkt alleen als ALLE relevante logs snel en makkelijk beschikbaar, toegankelijk en zoekbaar zijn.
Of met een SIEM, waarbij in duidelijke context sneller verschil tussen false & positive te geven is.

[1] (wikipedia) 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.

Retentie
Garantie dat logevents bewaart worden voor een bepaalde termijn, maar ook niet langer dan dat. Dus als de tijd verstreken is, is de logregel ook niet meer beschikbaar.

3.2 Controle op logs: Een voorbeeld proces

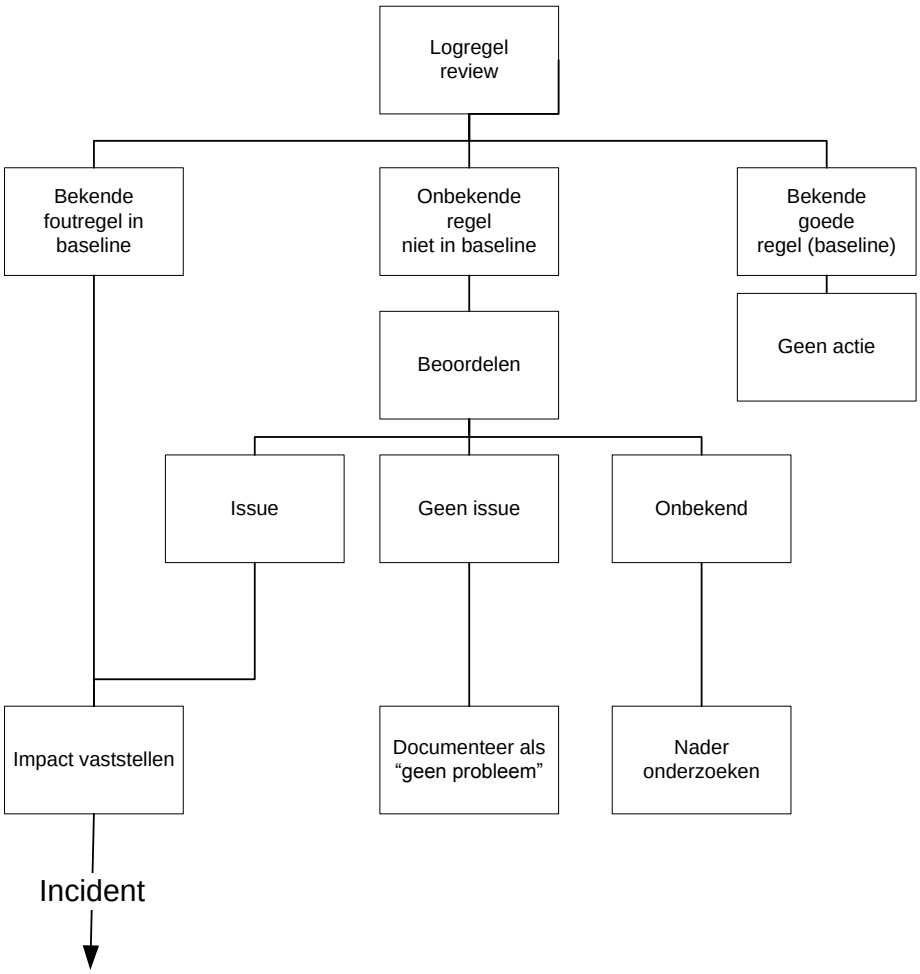
Om een indruk te geven van de hoeveelheid stappen die doorlopen kunnen worden bij het controleren van logregels, is hieronder een voorbeeld van een controle proces globaal uitgewerkt als best practice. Het bevat alle onderdelen die benodigd kunnen zijn bij het beoordelen van logregels. Dit proces kan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

Na het opbouwen van de BIG kan gestart worden met de (dagelijkse) controle activiteiten van de logs.

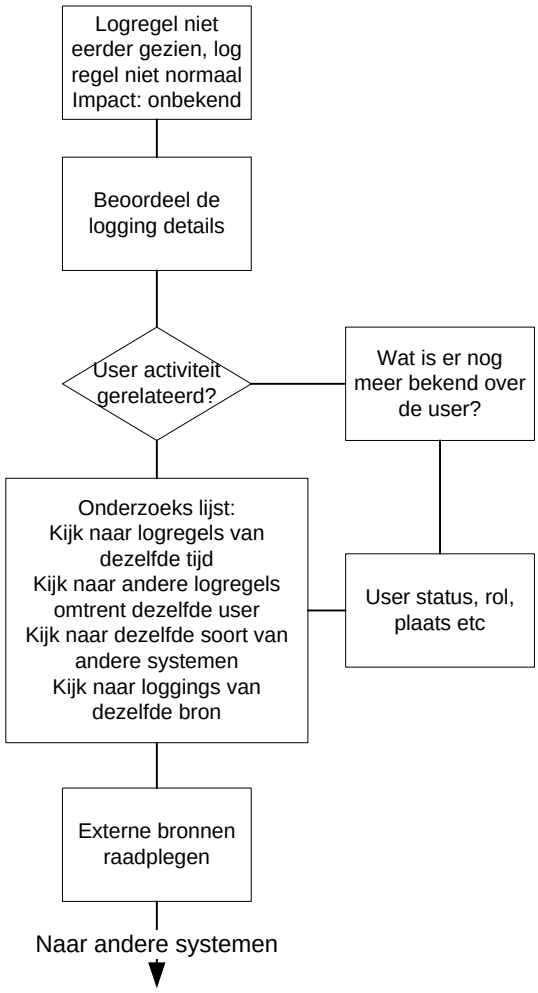
Analyse en onderzoek



De eerste stappen bij het beoordelen van de log is het doen van analyse en onderzoek. Bij deze analyse worden logregels vergeleken tegen de Baseline. Bekende foutregels in de Baseline worden na het bepalen van de impact 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 Baseline 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.

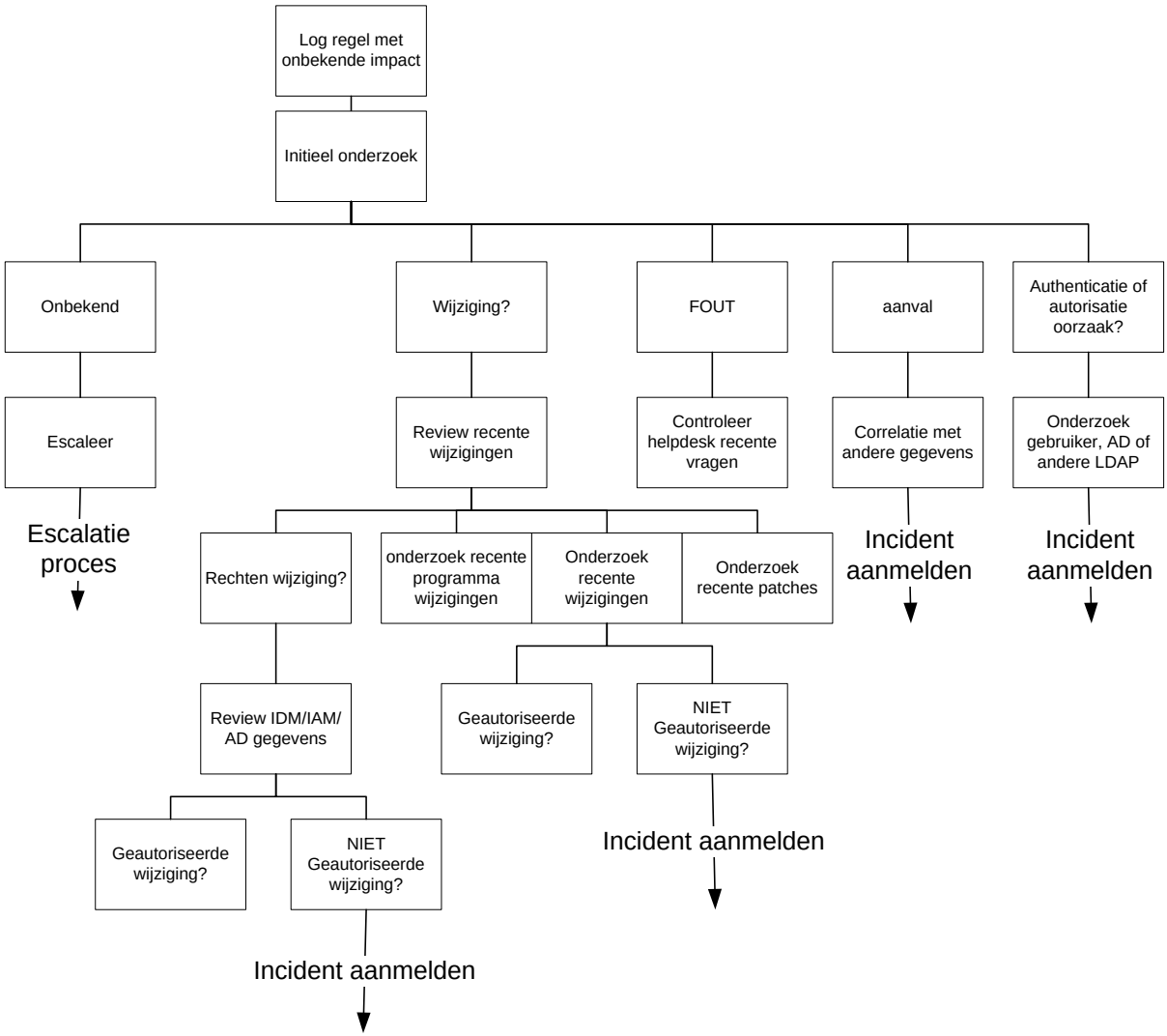
Logregel initieel onderzoek en user onderzoek



De logregels uit de eerdere stappen die nog niet eerder gezien zijn: De logregel is niet normaal en de impact is onbekend, worden hier 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, en er wordt tevens gezocht in andere logs rond hetzelfde tijdstip als dat nodig is. Documenteer alle gevonden gegevens voor verder onderzoek.

De volgende stap is het raadplegen van externe bronnen.

Raadplegen (externe) bronnen

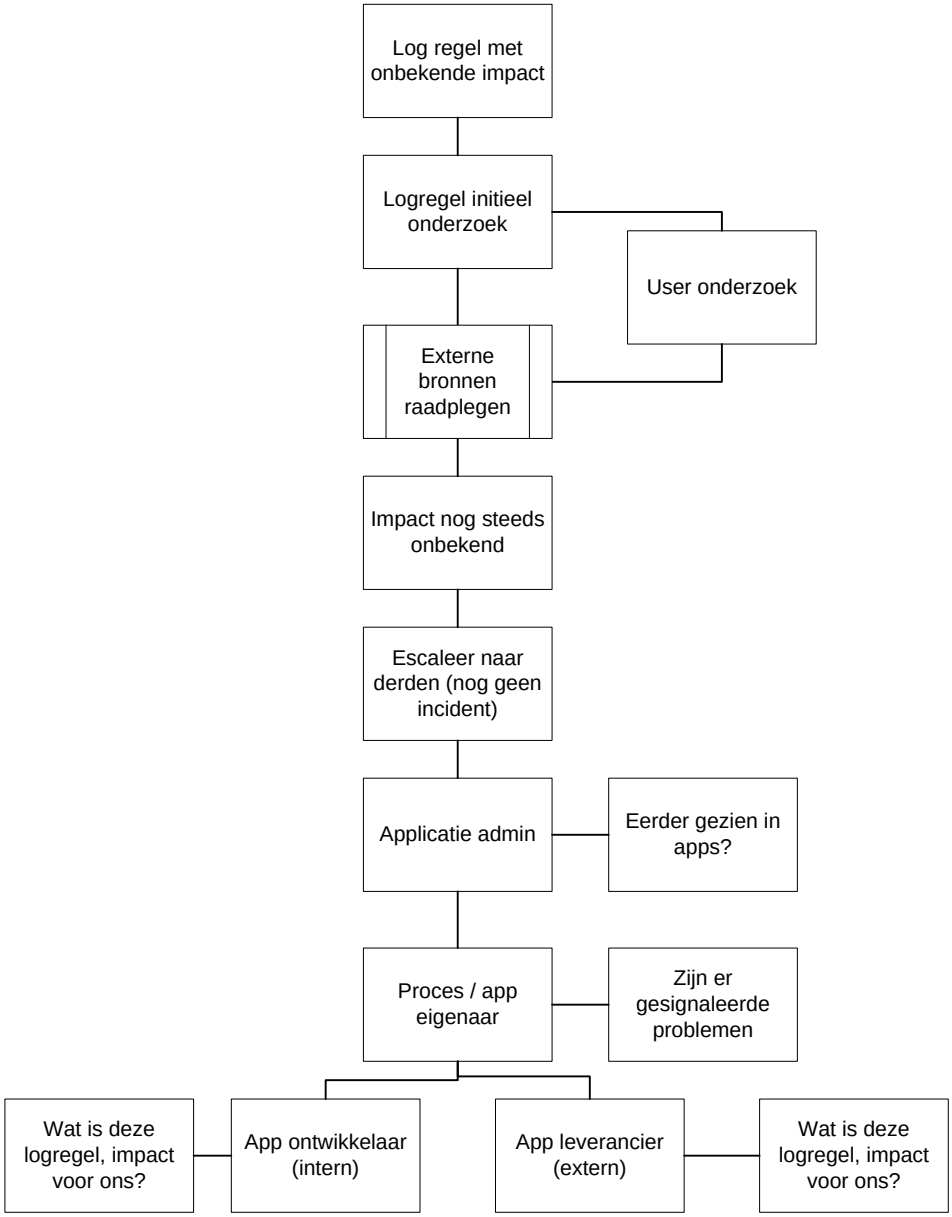


Het basisidee van deze procedure is het identificeren van informatiebronnen waar verder gezocht kan worden, gebaseerd op het type uitzondering van de logregel en vervolgens om het effect en de vereiste acties (indien aanwezig) te identificeren.
De procedure start met de identificatie van de aard van de vermelding in de logregel en daarbij worden vervolgens de relevante informatiebronnen geraadpleegd. De plaat hierboven is niet uitputtend.

Wanneer de logboekvermelding beschouwd kan worden als een indicatie van een (ernstig) probleem wordt overgegaan naar het Incident Response Proces, zie hoofdstuk 2.2 van het document. Dit proces is een apart product van de IBD.

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.

Overzicht proces controleren logregels



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

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. Het doel van dit interview is om te ontdekken of met de juiste mensen gesproken wordt die kennis hebben van de betekenis van de logregel, die kunnen helpen bij de impact bepaling en de juiste stappen of acties kunnen vaststellen om met de logregel en het geconstateerde om te gaan. Denk bij deze personen aan bijvoorbeeld de applicatiebeheerders/administrators of de eigenaar van de applicatie.

De laatste stap is dat de ontwikkelaar van de applicatie geraadpleegd wordt 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.

3.3 Bewijsvoering

Een belangrijk onderdeel van de review van de log is om ervoor te zorgen dat er voldoende bewijs is van het gevolgde proces, de implementatie van de gevolgde stappen en het gevonden resultaat. Dit is noodzakelijk als de logging-issues moeten dienen als bewijs indien er bijvoorbeeld aangifte wordt gedaan. Het goede nieuws hier is dat dezelfde gegevens kunnen worden gebruikt die ook nodig zijn voor de rapportage aan het management over de logging en log review-processen.

Welke documentatie is er nodig voor bewijsvoering:

1. Het hebben van en het toereikend zijn van de logging.
2. Het hebben van log review-processen en de implementatie ervan.
3. Exception Handling Proces en de uitvoering ervan.

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:

1. Gedocumenteerd logging-beleid, dat zowel ingaat op het registreren van gebeurtenissen als de gelogde details.
2. Beschrijving van de configuratie van systeem- en applicatie-logging op basis van het logging-beleid.
3. De geproduceerde logging-bestanden van de applicaties op basis van het beleid.

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:

1. Gedocumenteerd logging-beleid, dat ook de beoordeling van de log voorschrijft.
2. Gedocumenteerde operationele procedures, waarin de exacte stappen zijn beschreven voor het beoordelen van de logs.
3. Logboeken van logbeoordelingstaken die zijn uitgevoerd door het personeel (dit kan soms ook door Tooling worden verzorgd). Het gaat hier dus om ‘log beoordelingslog’.
4. Verslagen van het onderzoeken van uitzonderingen kunnen dienen als indirect bewijs dat de beoordeling van de log heeft plaatsgevonden (volgende paragraaf).

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 logging-beleid, 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

Logboek-bewijs van onderzoeks uitzonderingen (Exception of Investigations), waarin de uitzonderingen tijdens de dagelijkse beoordeling zijn gemarkeerd. Terwijl hetzelfde logboek wordt gehanteerd in het incident verwerkingsproces (zie Incident Response en Coördinatie, IBD), wordt het in dit document gebruikt als bewijs van naleving. 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 hun resultaten), et cetera.
Het volgende hoofdstuk beschrijft de inhoud van de registratie in het logboek.

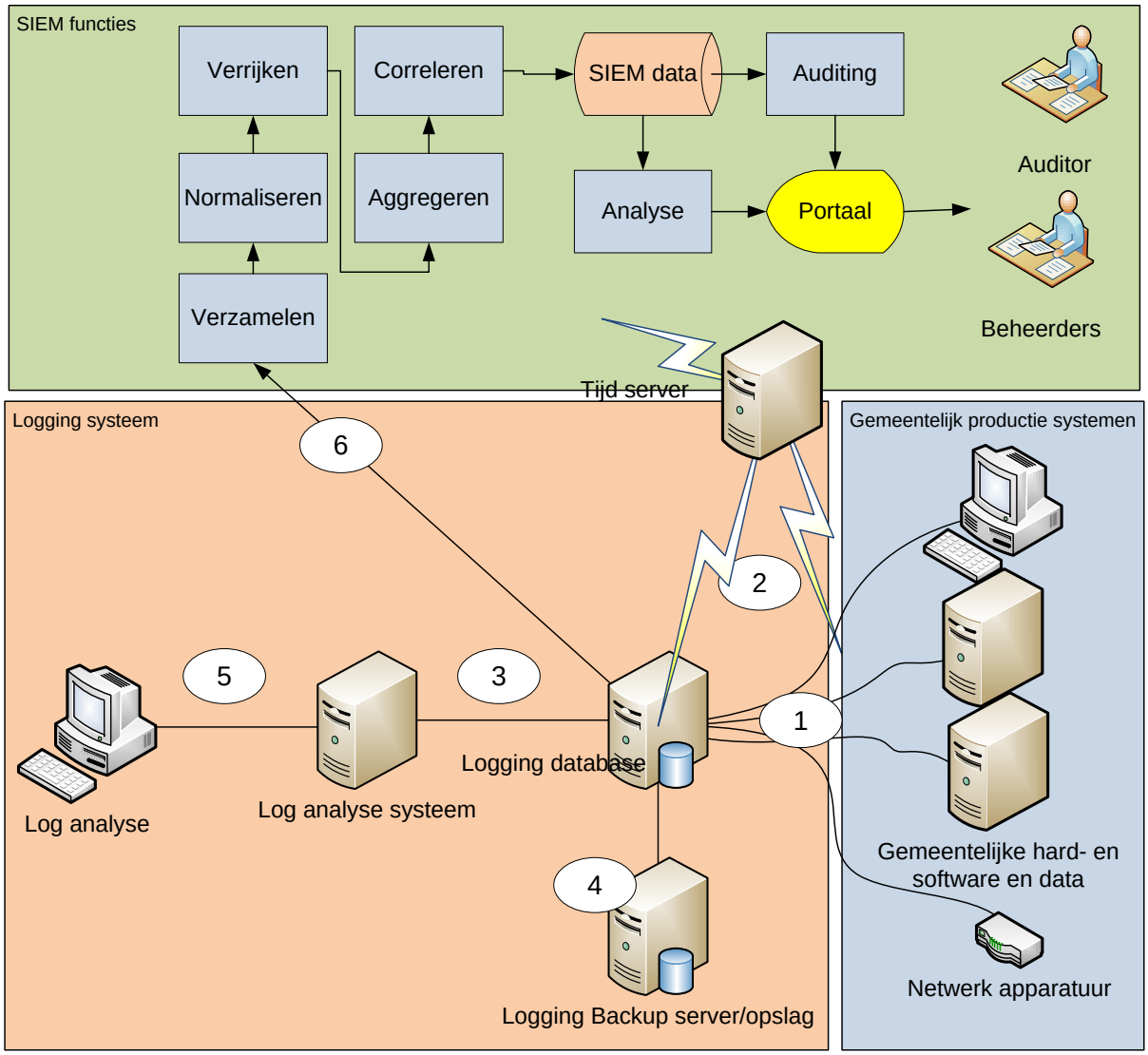
Een registratie in het logboek moet het volgende bevatten:

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).

3.4 Security Information and Event Management (SIEM)

SIEM 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, maar nu aangevuld met SIEM-functies.

SIEM heeft pas zin wanneer er een goede logging basis is, er dienen goede 'use cases' te zijn die het nodig hebben en er dient ook geïnvesteerd te worden in capaciteit om naar het SIEM-scherm te kijken.
Ook SIEM gaat uit van een vorm van baselinen, in dit geval het opbouwen van een context. Daarna kan er realtime worden geanalyseerd tegen de opgebouwde context. Context is bijvoorbeeld een lijst met ICT-beheerders uit de active directory of een lijst met bekende gebruikers die van buiten de gemeente mogen inloggen.

4 Bijlage 1: Logging-beleid gemeente <gemeentenaam>

4.1 Beleidsuitgangspunten Logging gemeente <gemeentenaam>

Ten behoeve van de beveiliging van informatie is er een logging-beleid voor alle gemeentelijke ICT-voorzieningen. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie tot logging genomen moeten worden binnen de gemeente.

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

4.2 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 BIG 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 gemeente 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 van de gemeente.

4.3 Controle van het beleid op systeemgebruik

Er zijn binnen de gemeente 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 resetent, 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.

4.4 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 behoren 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).

4.5 Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van de gemeente 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 burgemeester en wethouders van *[gemeente]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____

5 Bijlage 2: Gemeentelijke communicatie over logging van toegang tot en gebruik van systemen

Logging

De gemeente heeft rapportages ontwikkeld omtrent de logging van het gebruik van gemeentelijke systemen. De gemeente is verplicht om gegevens te loggen waarmee het gebruik van applicaties per medewerker van de gemeente 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, overzichtenen 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 gemeentelijke eindgebruikers van systemen moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met gemeentelijke 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 gemeentelijke 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 wordt voorgesteld om de gegevens over het gebruik van gemeentelijke applicaties eens per drie maanden te laten uitvragen.
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.

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**