Auditing Hansken

Zie ook:

- Audit logging
- HBACKLOG-16 - Getting issue details... STATUS

Juridische Achtergrond

Interpretaties en aannames

Auditlogging is een wettelijke verplichting op basis van de Algemene Verordening Gegevensbescherming (AVG) en Wet Politiegegevens (Wpg). In de AVG wordt logging niet expliciet vermeld maar is het meer een logisch gevolg wil voldaan kunnen worden aan de verplichtingen. In de Wpg wordt logging wel genoemd, maar de precieze invulling hiervan is nog in concept (Artikel 32a Wpg). De primaire doelgroep is de Privacy Officer, maar ook de CISO zal de resultaten in moeten kunnen zien.

Uit de PIA blijkt, afhankelijk van het gebruik van Hansken, dat zowel de AVG als de WPG van toepassing kunnen zijn We hebben niet kunnen vaststellen welke wanneer van toepassing is, maar het lijkt aannemelijk dat voor Hansken gebruikers de AVG van toepassing is, en dat op zaakdata meestal (zo niet altijd) Wpg van toepassing is (en anders de AVG). De reden om dit laatste (Wpg voor zaakdata) aan te nemen is dat binnen de AVG rechten gedefinieerd zijn van mensen wiens gegevens in systemen staan opgeslagen. Deze rechten houden in bijvoorbeeld het recht om te weten of en welke gegevens er van jezelf zijn opgeslagen, en het recht om deze gegevens te laten aanpassen of verwijderen. Uiteraard hebben de mensen wiens gegevens zijn opgeslagen in zaakdata in Hansken deze rechten niet. Dit leidt tot de aanname dat hier de WPG van toepassing is. Dit komt erop neer dat personen wiens gegevens in zaakdata in Hansken staat opgeslagen minder recht op privacy hebben. Dit maakt het aannemelijk dat het toezicht op het gebruik van deze gegevens (mogelijk gemaakt door auditlogging) van extra groot belang is.

Voor de implementatie van auditlogging in Hansken zijn bovenstaande overwegingen echter niet van belang, omdat er hier een concreter aangrijpingspunt is, namelijk de privacyverklaring op de website van NFI.

Op de homepage van het NFI staat in de privacyverklaring hoe NFI omgaat met persoonsgegevens. Andere ketenpartners zullen soortgelijke verplichtingen hebben.

De stukken die letterlijk uit Privacyverklaring, BIO en de daarin genoemde documenten zijn overgenomen is weergegeven in blauw.

Privacyverklaring

De informatie met betrekking tot auditlogging staan in paragrafen 7 en 8

-- begin citaat uit privacyverklaring

7. Hoe beveiligt het NFI persoonsgegevens?

Het NFI neemt maatregelen voor een passende beveiliging van uw persoonsgegevens. Voor de informatiebeveiliging van het NFI gelden de voorschriften en standaarden van de Rijksoverheid voor informatiebeveiliging Baseline Informatiebeveiliging Overheid (BIO). Persoonsgegevens worden vertrouwelijk behandeld. Dat wil zeggen dat het NFI ervoor zorgt dat alleen personen met de juiste bevoegdheden én een geheimhoudingsplicht persoonsgegevens kunnen verwerken.
Handelingen van medewerkers in systemen van het NFI worden gelogd. We houden bij wie welke handeling op welk tijdstip uitvoert in een logbestand. De logging wordt periodiek beoordeeld. Het NFI is aangesloten op het Nationaal Detectie Netwerk om vroegtijdig cybersecurity risico's te onderkennen en passende maatregelen te nemen.

8. Hoe lang bewaart het NFI de persoonsgegevens?

...
De bewaartermijn voor logging-gegevens is gerelateerd aan de uit te voeren kwaliteitscontroles en uit te voeren audits. Deze bedraagt standaard 2 jaar.

-- einde citaat

Het NFI heeft dus de verantwoordelijkheid om ervoor te zorgen dat alleen de juiste personen de persoonsgegevens in Hansken kunnen verwerken. De voorschriften en standaarden gesteld in de BIO zijn hierbij van kracht. Handelingen worden gelogd. Maar naast de technische implementatie van logging is het ook belangrijk dat deze logs periodiek worden beoordeeld. Wat er nodig is aan logging is verder uitgewerkt in de BIO.

Baseline Informatiebeveiliging Overheid (BIO)

In de privacyverklaring wordt gewezen naar de BIO. Hier zijn de relevante stukken voor auditlogging beschreven in paragraaf 12.4.

-- begin citaat uit BIO

12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1	1	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Proceseigenaar Dienstenleverancier
		Handreiking: Loggingbeleid	
		Handreiking: NCSC-handreiking detectie-oplossingen	
12.4.1.1	1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	
12.4.1.2	1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	
12.4.1.3	2	De informatie verwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties), die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
12.4.1.4	2	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	
12.4.1.5	2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	

12.4.2	1	**Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Dienstenleverancier
12.4.2.1	1	Er is een overzicht van logbestanden die worden gegenereerd.	
12.4.2.2	1	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	
12.4.2.3	2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	
12.4.2.4	2	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	

12.4.3	1	**Logbestanden van beheerders en operators** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Dienstenleverancier

12.4.4	1	**Kloksynchronisatie** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Dienstenleverancier

-- einde citaat

De eisen aan een logregel staan in 12.4.1.1 en 12.4.1.2. Het gebruik van een SIEM en/of SOC is verplicht. Verder staan er een aantal eisen aan de SIEM. Er moet een audit procedure worden ingericht. Bovendien wordt er expliciet bij stilgestaan dat activiteiten van beheerders en operators moeten worden gelogd en dat klokken gesynchroniseerd moeten zijn.

De eisen aan een logregel zijn hier redelijk abstract gespecificeerd. Er wordt verwezen naar een handreiking loggingbeleid waarin een voorbeeld wordt gegeven wat goede eisen aan logging zouden kunnen zijn.

Handreiking logging

De handreiking logging is *een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)* uitgegeven door de Informatiebeveiligingsdienst voor gemeenten (IBD). Het is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO), met als doel informatiebeveiligingsmaatregelen met betrekking tot logging en controle uit te werken en daarbij handreikingen te geven voor het logging-beleid en logging-procedures.

Er wordt hier onderscheid gemaakt in:

- **Technische logging:** Het doel is vaststellen of informatiesystemen correct worden gebruikt, goed worden beheerd en functioneren conform de gestelde eisen in bijvoorbeeld een SLA. Hier 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.
- **Audit logging:** Het doel is het vastleggen van activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen ten behoeve van toekomstig onderzoek en toegangscontrole

Paragraaf 2.5 beschrijft de inhoud van log logregel

2.5. Inhoud van een log
In de BIO 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
- 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

Paragraaf 2.8 beschrijft de keuzes wat te doen bij uitval van de logging

- De component normaal te laten functioneren en geen logging opslaan
- De component lokaal te laten loggen en later de logging te synchroniseren
- De component acuut uit productie laten halen

In bijlage 1: *Logging-beleid gemeente <gemeentenaam>* wordt de inhoud van een logregel vervolgens nog verder uitgewerkt:

Een logregel bevat minimaal:

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

Context van Hansken auditing binnen het totale zaaksonderzoek

Hansken is niet de enige tool die gebruikt wordt bij het analyseren van bewijsmateriaal. Veruit de meeste andere tools zoals Sleuthkit beschikken niet over deze audit functionaliteit. Er mag aangenomen worden dat de meeste personen die over Hansken beschikken ook beschikker over meerdere andere forensische tools. Dus zelfs als Hansken de auditlogging geheel op orde heeft dan zijn er nog talloze manieren voor kwaadwillenden om dezelfde data in te zien zonder dat dit geaudit wordt. Dit is zeker geen reden om auditlogging niet te implementeren, maar kan een argument zijn in de discussie hoe "mooi" of volledig de auditlogging in Hansken moet zijn.

Criteria voor een logregel

Dit was (hbacklog-16):

Iedere logregel bevat tenminste:

1. identiteit van de persoon die persoongegevens heeft geraadpleegd of bekend heeft gemaakt moet worden geregistreerd
2. datum en tijdstip
3. identiteit ontvangers (bij verstrekken van data en doorgiften)
4. volledige nieuwe waarde???
5. input van systeem
6. resultaat van systeem (niet inhoudelijk het antwoord)
7. Project ID Hansken

Nieuw voorstel

Iedere logregel bevat tenminste:

1. Een unieke ID voor deze gebruikersactie - Rationale: zodat er gemakkelijk naar gerefereerd kan worden door de privacy officer. Waarschijnlijk is dit al standaard geregeld in iedere gangbare SIEM.
2. Project ID Hansken - Rationale: een gemakkelijke eerste indicatie waar het om draait en mogelijkheid tot filteren
3. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID, maar geen "directe persoonsgegevens" zoals ??? - Rationale: BIO 12.4.1.1 & Logging - een handreiking voor JenV: waarin staat dat geen "directe persoonsgegevens" worden gelogd. Vraag: Dit zal de ID zijn die de identity provider teruggeeft aan Hansken. Als de gebruikersnaam "voornaam.achternaam", zou dit dan niet in de log mogen komen? Check met 10.2.e
4. Indicator vanaf waar de gebruiker toegang had tot het systeem, bijvoorbeeld een IP adres of host naam - Rationale: BIO 12.4.1.1 *een logregel bevat minimaal het gebruikte apparaat* & Handreiking logging *Waar mogelijk de identiteit van het werkstation of de locatie*
    1. en met welke "signature" dit gebeurde - Rationale: zodat nader vastgesteld kan worden of/welke tools gebruikt zijn
5. De datum en het tijdstip van de gebeurtenis - Rationale BIO 12.4.1.1 *een logregel bevat minimaal een datum en tijdstip van de gebeurtenis*
6. Het object ~~en de inhoud van het object~~ waarop de handeling werd uitgevoerd - Rationale: Handreiking logging *Het object waarop de handeling werd uitgevoerd* & Rationale voor het loggen van de inhoud van het object is dat wanneer dit niet gedaan wordt het weinig zin heeft om het resultaat van de handeling (zoals genoemd in BIO 12.4.1.1) op te slaan.

7. Het type actie, bijvoorbeeld aanmaken, opvragen, poging tot opvragen, wijzigen, poging tot wijzigen, verwijderen, poging tot verwijderen, zoeken - Rationale: handig zoeken door privacy officer & het beleidskader logging van de politie verwijst hier ook naar (CRUD)
8. Het resultaat van de handeling; bijvoorbeeld: gelukt of niet - Rationale: BIO 12.4.1.1 *een logregel bevat minimaal het resultaat van de handeling* NB het beleidskader logging van de politie noemt hier *Bij voorkeur worden deze resultaten niet via de logging vastgelegd, maar kunnen deze via de opslag van het systeem gereproduceerd worden.*
9. Informatie over het exporteren van informatie uit Hansken (indien van toepassing), inclusief de identiteit van de ontvanger, zoals verstrekken van data en doorgiften - Rationale: Wpg artikel 32a, *verstrekking onder meer in de vorm van doorgiften*
10. De handeling, bijvoorbeeld filter of zoekterm (indien van toepassing) - Rationale: Handreiking logging *Persoonsgegevens (of enige andere zoeksleutel) waarvan gegevens worden opgevraagd. Dit wordt als actie geregistreerd*

Het meeste van deze lijst komt direct voort uit wettelijke verplichtingen. De volgende punten zijn keuzes:

- Het loggen van de signature (punt 4)
- Het loggen van de inhoud van een object (punt 6)
- Het type actie (punt 7)

Voorbeeldlog

Voorbeeld: raadplegen informatie

```
Log ID           10000000123
Hansken project  ID 11
Host             156.45.200.12 <Mozilla header, ...>
Gebruiker        jmodaal
Tijd             2020-04-08 20:11:04.500
Object           traceUUID
~~Object inhoud    <Het spoor zelf>~~
Actie type       Read
Actie resultaat  Gelukt
Geexporteerd     -
Zoektermen       -
```

Voorbeeld: zoeken

```
Log ID           10000000124
Hansken project  ID 11
Host             156.45.200.12 <Mozilla header, ...>
Gebruiker        jmodaal
Tijd             2020-04-08 20:12:34.330
Object           -
Object inhoud    -
Actie type       Search
Actie resultaat  Gelukt
Geexporteerd     -
Zoektermen       name = "B. Boef" && date created < 2015:01:01 && sort on time ascending (uit
http post data)
```

Voorbeeld: alle acties van gebruiker jmodaal op 2020-04-08

```
Tijd                        Actie type

2020-04-08 20:11:02.000     Login
2020-04-08 20:11:04.500     Read
2020-04-08 20:12:34.330     Search
2020-04-08 20:12:36.000     Logout
```

Voorbeeld: alle acties op spoor traceUUID

```
Tijd                        Actie type        Gebruiker
```

2020-04-08 20:11:04.500	Create	zoperator
2020-04-08 20:11:04.500	Read	jmodaal