[HBACKLOG-16] Hansken audit Logging Created: 09/Jul/19 Updated: 15/Apr/20

Status:	Accepted
Project:	Hansken Backlog
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Story	**Priority:**	High
Reporter:	10.2.e	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	PI1_DEV, PI1_FIOD, PI1_NVWA, Prog_Volw, Team_TZN		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Issue Links:	**Blocks**			
	is blocked by	HBACKLOG-53	Centrale logging	Accepted
Stakeholders:	ONDERHOUD			
Business description:	Als Privacy Officer en Security Officer Wil ik inzicht hebben in het gebruik van informatie via Hansken in zaaksonderzoeken Zodat ik bewijs van compliance (met AVG en WPG) kan leveren Zodat ik (ab)normaal gebruik kan signaleren onder andere met betrekking tot accounts en autorisaties Zodat ik forensisch bewijs heb na een incident Dit gaat niet om de borging van bewijsketens tbv forensisch zaakonderzoek			
T-Shirt estimation:	L (2 sprints)			

Description

Wat

Alleen gebruikersacties op software die NFI levert.

Inclusief aanpassingen van toegangsrechten voor zover dit in de meegeleverde Hansken AD wordt uitgevoerd.

Buiten scope: Activiteiten van systeembeheerders

Buiten scope: Implementeren SIEM

Chronologische auditlogging van gebruikersacties op de REST interface van Hansken, verstuurd naar een SIEM.

Aanname (te verifieren) NFI (FIG) gebruikt Splunk en deze kan als SIEM worden gebruikt. Zo niet dan moet een aparte SIEM worden gerealiseerd. Dit valt buiten deze feature.

In kaart brengen welke SIEM systemen worden gebruikt bij de ketenpartners navraag tijdens architectuurgroep week 16

Aansluiting mogelijk maken op SIEMs van FIOD en Politie. Als het goed is gebruik makend van een standaard protocol.

Waarom

Compliance met AVG, Wpg, BIO in eerste instantie alleen voor Nederlandse ketenpartners. Buitenlandse partners zouden eventueel andere eisen kunnen hebben maar die zijn hier niet meegenomen.

- Leveren bewijs van compliance (AVG inzageverzoek)
- Signaleren (ab)normaal gebruik, o.a. accounts, autorisaties
- Signaleren fouten en incidenten in systemen
- Als forensisch bewijs na een incident

Zie ook: Auditing Hansken; juridische achtergrond etc

Het technisch mogelijk maken om invulling te geven aan de volgende aanbevelingen zoals gedaan in de PIA Hansken:

- PIA 1 Periodieke audit op werkmethode Hansken
- PIA 6 inrichten adequate logging en monitoring van alle gebruikersactiviteiten + bewaartermijnen
- PIA 14 Logging van alle mutaties in de audittrail in Hansken + bewaartermijnen en monitoring op deze logging

Risico wanneer dit niet wordt geïmplementeerd: negatief advies bij ingebruikname Hansken van security en privacy officers.

Wpg, AVG, BIO vragen om een juiste implementatie van audit logging. Hansken heeft deze ondersteuning momenteel niet in productie. Dit wordt aangedragen door AVG, Wpg, en BIO checks als een kritisch punt wat op orde gebracht moet worden.

Beslissingen

Auditlogs worden niet in Hansken zelf opgeslagen maar in een externe SIEM.

Experts

- 10.2.e - Privacy officer NFI
- Secuirty officer NFI

- 10.2.e (beheer centraal logging systeem DBS)
- 10.2.e audit logging FIOD)

Afhankelijkheden

Acceptatie criteria

1. Iedere logregel bevat tenminste:
    1. Een unieke ID voor deze gebruikersactie
    2. Project ID Hansken
    3. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID, maar geen "directe persoonsgegevens" zoals ??? (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 en met welke "signature" (bijvoorbeeld browser header) dit gebeurde
    5. De datum en het tijdstip van de gebeurtenis
    6. Het object waarop de handeling werd uitgevoerd
    7. Het type actie, bijvoorbeeld aanmaken, opvragen, poging tot opvragen, wijzigen, poging tot wijzigen, verwijderen, poging tot verwijderen, zoeken
    8. Het resultaat van de handeling; bijvoorbeeld: gelukt of niet
    9. Informatie over het exporteren van informatie uit Hansken (indien van toepassing), inclusief de identiteit van de ontvanger, zoals verstrekken van data en doorgiften
    10. De handeling, bijvoorbeeld filter of zoekterm (indien van toepassing)

2. De volgende gebeurtenissen dienen gelogd te worden:
    1. Gebruik van functionele beheerfuncties, bijvoorbeeld het aanpassen van toegangsrechten voor zover dit in Hansken / Hansken AD wordt uitgevoerd
    2. Handelingen van gebruikers

3. Audit logs mogen niet inzichtelijk zijn voor systeembeheerders (geen onbevoegde toegang)

4. Audit logs worden opgeslagen in een SIEM:

5. Logging is integer: zolang logs binnen de applicatie van Hansken opgeslagen of verwerkt zijn, zijn de logs integer. Ook kan de integriteit van de logs nog worden afgeleid wanneer deze op een extern systeem zijn opgeslagen.

6. Audit logs mogen niet verloren gaan bij downtime van een gekoppeld systemen.

7. Minimale performance impact op applicatie vanuit gebruikersperspectief.

8. Instelbaar per organisatie wat te doen als er geen logging endpoints beschikbaar zijn (applicatie stoppen, logs queuen, of applicatie laten doordraaien)?

9. Documentatie is opgeleverd die beschrijft wat er op welke manier wordt gelogd ten behoeve van privacy officers van organisaties waar Hansken wordt gebruikt.

~~10. Gescheiden audit trails: Auditlogging gesplitst op basis van tenant, zodat de privacy officer van elke tenant alleen de logs ziet behorende bij zijn of haar organisatie~~ Opties: ondersteuning aparte SIEMs of aparte *stream* of is de eigenaar van de Hansken omgeving verantwoordelijk voor de auditing en is dus 1 SIEM genoeg? Voorlopig gaan we van dit laatste uit.

11. Wat te doen met embargo zaken? Gewoon auditen net als iedere andere zaak of moeten deze worden uitgesloten van auditlogging?

12. Wat te doen met account advocaat? Gewoon auditen net als iedere andere zaak of moeten deze worden uitgesloten van auditlogging?

Relevante documentatie

Voorbeeld hoe een auditlog er uit kan zien & juridische achtergrond achter auditing requirements: Auditing Hansken

Originele pagina met audit logging requirements en technische implementatie: Audit logging

Open punten

Comments

Comment by 10.2.e (DBS) [02/Oct/19]

Opmerking, zoals omschreven op 10.2.g kan de audit logging worden opgeslagen in een SIEM (Security information and event management)-systeem. Dit is software die bij de afnemer van Hansken is geïnstalleerd en is beheerd. Door het gebruik van een SIEM valt inzicht geven in audit logging en het beheer van de opslag buiten de verantwoordelijkheid van Hansken. Dit scheelt implementatietijd (Estimate: L)

Comment by 10.2.e DBS) [14/Apr/20]

- verplaatst naar HBACKLOG-121 -

Generated at Mon Apr 20 16:12:22 CEST 2020 b 10.2.e using Jira 10.2.g