

Reactie op PIA Hansken

Er hebben 2 PIA's plaatsgevonden:

- gebruik van Hansken t.b.v. ontwikkelingen aan zaakspecifieke forensische bibliotheken/Hansken (1A)
- gebruik van Hansken voor NFI zaakonderzoek (1B)

Uit deze PIA's zijn meerdere aanbevelingen gekomen:

Nr	Onderwerp	Voorgestelde maatregel	Belang	Verantwoordelijke partij	Maatregel
1	Transparantie /rechten betrokkenen	Periodieke audit op werkmethode Hansken	L	DBS business	Hansken: Auditfunctie toevoegen, al gestart DBS-1A: Overleg met FSE/DA over werkproces ontwikkeling nieuw software t.b.v. zaak DBS-1B: Hansken is yet-another tools die we gebruiken voor zaakonderzoek, de werkmethode moet dan breed geaudit worden. Probleem is dat we vrijwel alleen maatwerk uitvoeren, een werkmethode is dan lastig.
2		Update van het privacy statement op de NFI website	M	Privacy officer	Overleg met privacy-officer over statement mb.t. data-verwerking door DBS t.b.v. zaakonderzoek

DBS-1A: De data is enkel nodig voor de duur van het onderzoek, d.w.z. voor tijd die nodig is om de software-uitbreiding te realiseren. Daarna kan deze verwijderd worden. Vraag: Hoe zorgen we dat we een goede testset krijgen voor de ontwikkelde software? Dit kan niet op basis van de onderzochte zaakdata. Referentie-data creëren is niet altijd haalbaar.

DBS-1B: Dit is voor per se relevant binnen Hansken. De data staat namelijk op de zakenserver, een kopie staat in Hansken. Deze kopie kunnen we na afsluiten van de zaak direct verwijderen. Hier is nu geen beleid op.

4	Toegang en Autorisatie	Formalisieren van toegangsverlening tot zaakdata voor NFI medewerkers; dit geldt ook voor afmeldingen voor medewerkers die niet meer ingezet worden op een specifieke zaak	M	DBS business	Hansken: Auditfunctie toevoegen aan autorisatie management authorisaties beleggen bij zaak operator (ipv systemoperator) DBS: Authorisaties op Hansken vastleggen in een Inception-document DBS-18: Authorisaties in Hansken vangen niet de authorisaties op de zakenserver, dus ook na het intrekken van bevoegdheid en kunnen de onderzoeker s bij de data.
5		Inperken bevoegdheden tot de zgn. Experimenteer omgeving Hansken (niet kunnen beïnvloeden van beveiligingsopties)	H	DBS business	Algemeen: deze omgeving is momenteel NIET operationeel Hansken: Auditlogging op experimenteer omgeving, autoriseren tegen de autorisatie-service die ook in productie gebruikt wordt. Expliciete authorisaties op user-added data (die in productie tijdens onderzoek is toegevoegd).
6		Inrichting adequate logging en monitoring op logging van alle gebruikers activiteiten; en het bepalen van de bewaartermijn van de logging	H	Hansken ontwikkelgroep	Hansken: Auditfunctie toevoegen, monitoring via log-systeem (bv. SIEM)
7		Alle medewerkers die werken met Hansken moeten gescreend zijn	M	DBS business	Dit is al DBS-beleid

8		Inrichten van de beveiliging van uit Hansken geëxporteerde data c.q. het afschermen van de exportfunctie	H	DBS business en aanpassing implementatie handleiding door Hansken ontwikkelgroep	Hansken: voorkomen exportfunctie van objecten die geheimshoudersgegevens bevatten. DBS: Afschermen van de exportfunctie is geen optie en staat haaks op de functie van Hansken. DBS-1A: overleg met FSE/DA over lokale opslag van zaakdata, hier is nu volgens Harm geen beleid voor. DBS-1B: Gebruikers van Hansken hebben al toegang tot de zakenserver, dus tot alle data in een zaak. Beperkingen in Hansken helpen hier niet bij.
9	Datalekken	Input data door toeleveranciers versleuteld laten aanleveren	M	DBS business en in handleiding door Hansken ontwikkelgroep	Dit ligt buiten Hansken, de aanlevering loopt nu via de LE (blauwe kratten). DBS: afspraken maken met keten?
10		Extra verificatie op adres van ontvanger rapportage	M	DBS business	DBS-1A: geen rapportage, oplevering via release DBS-1B: verificatie gebeurt al in het schaduwproces
11		Opstellen van een verwerkersovereenkomst met OM/politie	M	DBS business	DBS: Is dit nodig? Bij expliciete opdracht lijkt me dit impliciet geregeld. RC is geen eigenaar van de data, bespreken met privacy-officer.

12	Betrouwbaarheid programmatuur	De programmatuur / modules onderwerpen aan aantoonbare testcycli, en waar mogelijk laten certificeren; formeel protocol opstellen	M	Hansken ontwikkelgroep	Hansken: Bebibliotheken beter testen en test coverage uitbreiden. Staat al op de backlog. Certificeren is niet mogelijk, eerder geprobeerd, maar niet mogelijk gepleken. Ook lastig met korte release-cycli.
13	Datakwaliteit	Toevoegen van maatregelen om de volledigheid en juistheid van het inlezen van aangeleverde data te waarborgen (bv door opnemen van hashtotals).	M	Hansken ontwikkelgroep	Hansken: funcite is beschikbaar om acquisitie- hash en hash van image in Hansken te vergelijken. DBS-1A: bespreken met FSE< minder belangrijk wat geen rapportage. data moet natuurlijk wel kloppen. DBS-1B: hash- vergelijkinge n zijn reeds onderdeel van de schaduwproc edure.
14	Onrechtmatig datagebruik	Inrichten monitoring op logging	H	DBS business	Zie punt 6
De aanpassingen IN Hansken na v. van de PIA's zijn opgenomen in		10.2 g			
10.2 g					

