Betreft: Evaluatie risicoanalyse Infectieradar RIVM (september 2020)
Datum : 8 september 2020
Aanwezig: (10)(2e), (10)(2e), (10)(2e), (10)(2e), (10)(2e), (10)(2e)

Inleiding

Na een uitgebreide risicoanalyse waarbij zowel de applicatie 'Infectieradar RIVM', de onderliggende infrastructuur en de processen onder de loep zijn genomen is er een document opgesteld dat de restrisico's (status 7 september 2020) opsomt ter beoordeling. Dit is het 'Aanvraagformulier risico-acceptatie – Infectieradar RIVM'.

Het aanvraagformulier heeft overigens een sterke focus op informatiebeveiliging. Privacyrisico's zijn in het aanvraagformulier nog onderbelicht maar zullen in dit document wel worden meegenomen. Het uitvoeren van een Privacy Impact Assessment heeft, gezien de huidige restrisico's, nog geen zin.

Doel van dit document is een onderbouwing van het oordeel dat gegeven is over het in productie nemen van de Infectieradar RIVM (versie september 2020), waarbij richtlijnen vanuit de BIO en (U)AVG leidend zijn.

Conclusie

Op basis van de restrisico's die zijn geïdentificeerd, voor zowel informatiebeveiliging als privacy, komen we tot de conclusie dat de huidige versie van 'Infectieradar RIVM' op dit moment **niet in productie** kan worden genomen zonder de in de volgende hoofstukken genoemde maatregelen geïmplementeerd te hebben.

Informatiebeveiliging

Enkele aanvullende vragen/notities vanuit het overleg:

- Indien een bijdragend proces in plaats van ondersteunend, verandert dit nog iets aan het beveiligingsniveau? Is dat al meegenomen?
  Antwoord: Deze aanpassing verandert niets aan het gewenste beveiligingsniveau (BBN2).
- Invullen gegevens voor kinderen? Dubieuze functionaliteit.
- R-schijf. Autorisaties en verwijderen. Hoe is dit geregeld?
  Antwoord: op basis van RIVM-account en conform het geldende RIVM IAM proces. Alleen onderzoekers die betrokken zijn bij het onderzoek waarvoor Infectieradar wordt ingezet hebben toegang.
- Pseudonimisatie zoals nu geregeld, ontoereikend voor dit niveau gegevens (P-risico hoog). Hoe gaan we dit beter regelen?
  Antwoord: vanuit privacy (10)(2e) is een mogelijke oplossing aangedragen in de vorm van een additionele 'hash database' waar de vertaling/versleuteling wordt opgeslagen en waarvoor afwijkende toegangsrechten gelden (andere administrators bijvoorbeeld). Deze optie zou onderzocht kunnen worden.

De volgende set aan restrisico's moet tenminste worden opgelost voordat de applicatie op een veilige en verantwoorde manier in productie kan worden genomen.

Restrisico's	Toelichting	Maatregelen
Applicatielogs voldoen niet aan de BIO-richtlijnen.	• Er is onvoldoende logging aanwezig om (forensisch) onderzoek mogelijk te maken bij eventuele incidenten/datalekken. • Er zijn 6 beheerders die toegang hebben tot alle data; acties kunnen in de Openshift omgeving echter niet herleid worden tot één individu. (toegang wordt wel gelogd). • Logfiles worden niet actief gemonitord. • Er wordt niet voldaan aan de BIO (12.4.1, 12.4.2, 12.4.3).	• De 'log events' in de applicatie uitbreiden met security gebeurtenissen conform aangeleverde specificatie. *Update 8-9 (15:00): Leverancier geeft aan dat applicatielogs gereed zullen zijn op 11-9 conform aangeleverde specificaties.* • Logfiles m.b.t. handelingen van administrators (te herleiden tot individu) uitbreiden en monitoren via RIVM SOC. • Logging inregelen conform art. 12.4 BIO en NEN 7513.

Accounts van onderzoekers zijn niet gekoppeld aan RIVM IAM, zoals beschreven in de PSA.	• Indien medewerkers van het RIVM-toegang moeten krijgen tot een applicatie, dient dat te gebeuren via het eigen RIVM-account (Active Directory/ Single Sign On). Dit om het Identity en Access Management (IAM) proces van RIVM te borgen.	• Single Sign On (2FA) realiseren voor onderzoekers die moeten inloggen op de Infectieradar (op basis van RIVM-account), zoals beschreven in de PSA. • Inregelen van beheer van toegangsrechten conform 9.2 BIO
De wachtwoorden van deelnemers zijn onvoldoende beschermd.	• Het toegepast algoritme om de wachtwoorden te versleutelen (Argon2) is verkeerd ingesteld.	• De variabele voor het aantal iteraties van het algoritme moet aangepast worden van 1 naar 4 door de leverancier.
Er is geen (onderhouds)contract met de leverancier (Coneno).	• Er is nergens vastgelegd of en hoe we na inproductiename van de Infectieradar verder samen gaan werken met de leverancier Coneno. Afspraken over onderhoud en eventueel intellectual property zijn nog niet gemaakt.	• Contract[1] opstellen met Coneno waarin de afspraken over eventuele verdere samenwerking worden vastgelegd conform BIO en AVG.
In het aanmeldformulier voor het onderzoek is geen controle aanwezig of er een mens of automatisch script de aanmelding invult.	• Normaal gesproken wordt een dergelijke kwetsbaarheid verholpen door gebruik te maken van een zgn. captcha oplossing (bewijs dat je een mens bent door het oplossen van een 'puzzel'). De gangbare oplossing is reCaptcha van Google. Hiervan is echter onduidelijk welke informatie nog meer wordt verzameld en wat daar vervolgens mee wordt gedaan. • Op dit moment is gekozen voor een alternatieve oplossing waarin binnen de applicatie een limiet gezet wordt op het aantal aanmeldingen dat mag worden gedaan in een bepaald	De anti-bot functionaliteit van de aanwezige (F5) netwerkapparatuur inschakelen om dergelijke scripts te detecteren en te blokkeren.

[1] Zie aanvullende informatie in bijlage A.

	tijdsframe (10 minuten). Hiermee loop je het risico dat als een aanvaller een script gebruikt voor aanmelden, de applicatie voor bepaalde tijd niet beschikbaar is voor anderen (Denial of Service).	
Sessie van deelnemer kan worden overgenomen in een zgn. 'Man in the Middle Attack'.	• Indien een deelnemer via een publiek wifinetwerkverbinding maakt met de Infectieradar, kan het netwerkverkeer worden afgeluisterd en kan het 'sessie cookie' buitgemaakt worden. Hiermee kan een aanvaller de sessie van de deelnemer overnemen. • Vanwege de manier waarop de netwerkapparatuur inkomende verbindingen afhandelt, is het op dit moment niet mogelijk om gebruik te maken van 'secure cookies'	• De aanwezige apparatuur zo configureren dat 'secure cookies' wel afgehandeld kunnen worden. *Dit komt de beveiliging van alle RIVM-websites ten goede.*

Privacy

In termen van privacy risico's voor degenen wiens persoonsgegevens worden verwerkt en voor het RIVM, volgt uit de IB-risicoanalyse dat

het RIVM onvoldoende passende technische en organisatorische maatregelen heeft getroffen en onvoldoende kan waarborgen en kan aantonen dat de verwerking Infectieradar.nl in overeenstemming is met de wet

Restrisico	***Toelichting***	***Maatregel***
Kenmerken verwerking		
Beschrijving verwerking in PIA, Racc, PSA, Dataflowchart; site' publicitaire uitingen	*Er is geen consistentie in de teksten. Mist welbepaaldheid.*	*Teksten aanpassen.*
De verwerking: Infectieradar.nl; studie; vragenlijsten enz.	Afbakenen qua omvang en tijd (welbepaald maken). Bij wijziging van vragenlijst of technische oplossing dient een nieuwe risicoanalyse te worden uitgevoerd.	Procedure opstellen (die ook betrekking heeft op het geval van het combineren van de onderzoeksresultaten zodanig dat gegevens weer herleidbaar zijn)
Documentatie/ aantoonbaarheid (projectdocumentatie)	Er ontbreekt een inventarislijst (overzicht) van de uitgevoerde stappen en bevindingen van	Documentatie op orde zodat gemaakte keuzes inzichtelijk kunnen worden gemaakt een

	het doorlopen IRM-proces	compliance niveau aangetoond kan worden
Rechtmatigheid		
Privacyverklaring	Privacyverklaring is nog niet toegesneden op de huidige verwerking (Formdesk verhaal)	*Privacyverklaring aanpassen op de huidige verwerking*

Privacyverklaring aanpassen aan nieuwe verwerkingsgrondslag (geen toestemming)	Privacyverklaring is nog niet aangepast (mogelijk indien vastgesteld dat pseudonimisatie voldoende niveau heeft om nieuwe verwerkingsgrondslag te hanteren)	*Niveau pseudonimisatie optimaliseren (technisch & qua beheermaatregelen). Indien geregeld, wettelijke taak als verwerkingsgrondslag hanteren.*
Ouders/ voogd -kinderen (één account voor alle gezinsleden)	Risicovol dat er onder één account informatie van meerdere gezinsleden kan worden opgegeven (kinderen 12-16 enz.)	n.t.b.
Emailherinnering	Toestemming burger vereist	Opt out & opt in regelen
Nieuwsbrief	Toestemming burger vereist	Opt out & opt in regelen
Bewaartermijn	Niet genoemd	*Bewaartermijn documenten/dataset vaststellen en procedure opstellen zodat dit ook technisch gerealiseerd wordt*
Bewaartermijn	Vaststellen hoe om te gaan met bewaartermijnen in het licht van Corona als hotspot	*Procedure opstellen hoe hier mee te gaan*
Delen gegevens/ herleidbaarheid gegevens tot personen		Procedure opstellen
Delen gegevens/ in samenwerkingsverband met Influenzanet		Procedure opstellen
Publicatie van onderzoeksresultaten		Procedure opstellen
Pseudonimisatie zoals nu geregeld, is ontoereikend voor dit niveau gegevens (P-risico hoog).		Hoger niveau van pseudonimisatie inregelen.
Uitoefenen rechten van betrokken		***Procedure opstellen***
Rechten van betrokkenen		*Procedure opstellen* Technische en organisatorische stappen inregelen om gehoor te geven aan de verschillende soorten verzoeken rechten van betrokkenen *Capaciteit regelen voor het (administratief en juridisch) afhandelen van verzoeken van betrokkenen.*

Screenflows/ Informatieplicht		
Omschrijving onderzoek & doel van het onderzoek	-Consistentie met documentatie PIA, PSA enz. Vermijden van dubbelzinnigheid	
Teksten actieve handelingen		Review teksten
Duidelijke verwijzing naar de privacyverklaring		Checken screenflow
Actieve handeling waaruit blijkt dat de burger de privacyverklaring heeft gelezen		Checken of je pas het aan het onderzoek kan deelnemen wanneer je deze actieve handeling hebt verricht
Actieve handeling waaruit blijkt dat de burger de privacyverklaring heeft gelezen	Aanvinken moet mogelijk zijn	***Aanvinken mogelijk maken***
Link naar Twitter, Facebook, Instagram, You Tube, Linkedin (NIEUW in versie 0.11.0)	Uit deze functionaliteit vloeien privacy risico's voor burgers uit	Privacy risico's inventariseren en besluiten óf het wenselijk is om deze functionaliteit aan te bieden. Zo ja, dan ook privacy statement hier op aan passen
Disclaimer (1) vrijwilligheid	*Vrijwilligheid burger moet ondubbelzinnig worden vermeld*	*Disclaimer vermelden*
Disclaimer (2) geen medische website	*Ondubbelzinnig vermelden dat het niet om een medische website gaat*	*Disclaimer vermelden*
Toestemmingsverklaring		
Herinneringsmail	Toestemming/ opt in	
Nieuwsbrief	Toestemming/ opt out	
Herinneringsmail	Afmelden voor	
Nieuwsbrief	Afmelden voor	
Actieve verklaring 16 jaar en ouder	Apart kunnen aanvinken	
Influenzanet samenwerkingsverband	Datasharingsovereenkomst, indien gegevens worden gedeeld	
Leverancier Coneno	Overeenkomst van opdracht en overige afspraken omtrent beschermingsniveau (IB&P) in verband met (door)ontwikkeling software en onderhoud ervan	

Bijlage A Aanvullende informatie

Onderwerpen die besproken kunnen worden met de leverancier (Coneno) en vast te leggen in een overeenkomst:

1. De diensten (welke zij doen en welke wij doen)
2. De servicelevels
3. Continuïteit van de dienstverlening
4. Overdrachtsovereenkomst (transitie)
5. Sub contracten (wel of niet toegestaan)
6. Kwaliteitscriteria
7. Gebruikte technologie
8. Acceptatieprocedures
9. Exit procedure en consequenties van een exit
10. Tijdslijnen
11. Auteursrechten (intellectueel eigendom)
12. Vertrouwelijkheid en publiciteit
13. Verzekering en aansprakelijkheid
14. Force majeur
15. Audit
16. Wijzigingsprocedure m.b.t. het contract
17. Databescherming en privacy
18. Procedure voor het oplossen van geschillen
19. Testprocedures en strategie