Classificatie: RIVM Vertrouwelijk

RIVM Risicoanalyse

CovApp

Auteur: 5.1.2e

Datum: 15 jan 2021

Versie: 0.3

Inhoud

MANAGEMENTSAMENVATTING

Managementsamenvatting

- ✓ De deelnemers van het MORGEN project en van de Doetinchem Cohort Studie (DCS) worden gevraagd mee te doen aan aanvullend onderzoek over Covid-19. Ze krijgen maandelijks vragen over symptomen. Het doel van dit onderzoek is om meer te weten te komen over Covid-19 en de impact hiervan op de gezondheid en leefstijl.
- ✓ Het proces is geclassificeerd als 'bijdragend'. De data en het onderzoek dat uit dit proces volgt kan bijdragen aan het krijgen van een beter inzicht in de impact van COVID-19 op de gezondheid en leefstijl.
- ✓ De BIV van de informatiesystemen is vastgesteld als Laag Midden Midden.
- ✓ De CovApp wordt geleverd door YourResearch. Medewerker RIVM logt in bij YourResearch om de ingevoerde gegevens van de cliënten op te halen.
- ✓ Er is op 18 november 2020 contact geweest met 5.1.2e van Universiteit Utrecht over security van de CovApp 5.1.2e deelde mee dat Universiteit Utrecht een dataclassificatie en een risicoanalyse heeft uitgevoerd. Er is ook een pentest uitgevoerd door de fa. S-Unit.
- ✓ Er waren bevindingen op het gebied van wachtwoord versleuteling op Android en IOS, hardening, kwetsbaarheden management en ontwikkelmethode van YourResearch.
- ✓ 5.1.2e heeft voor UU een voorlopig positief advies gegeven voor het gebruik van de app.
- ✓ Er is op 7 en 12 januari bij RIVM ook een risicoanalyse uitgevoerd waarbij 12 dreigingen naar boven gekomen zijn. Behalve 1 dreiging (ziektegolf door besmetting met virus of bacterie, de huidige corona pandemie) hebben deze dreigingen een kans laag zodat hiervoor geen maatregelen nodig zijn.
- ✓ Voor de corona pandemie is als maatregel gekozen: Regel vervanging van personeel bij RIVM en bij YourResearch.

Overzicht huidige risico's

Uit de risicoanalyse zijn de volgende risico's naar voren gekomen en samengevoegd in onderstaande heatmap. De risicowaardering is gebaseerd op de BIV-impact classificatie uit de Quickscan BIO en de kansbepaling uit de dreigingensessie.

impact \ kans	1 <1 keer per 10 jaar	2 Minimaal 1 keer per 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 hoog					
2 midden	R02 R04 R07 R10	R01 R05	12		
1 laag	R03 R06 R09 R11	R08			

AANPAK RISICOANALYSE

FA

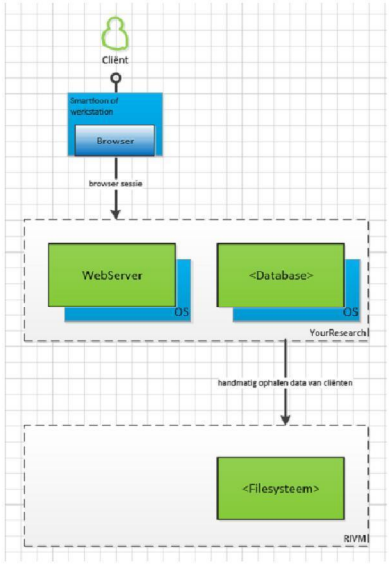
Fase I	Fase II	Fase III	Fase IV	Fase V
CONTEXT	IMPACT	DREIGINGEN	WEERBAARHEID	RAPPORTAGE
Situatieschets van locaties, systemen, informatie & toegang	*Classificatie van proces, systeem en informatie (BIV) & BBN niveau*	*Inzicht in dreigingen & kwetsbaarheden, de consequenties en kans dat het zich voordoet*	*Inventarisatie huidige maatregelen & voorstel aanvullende maatregelen*	*Vastlegging van risico's, maatregelen & terugkoppeling*

Fase 1: Context

Context

Voor het RIVM zou de MORGEN en DCS populatie gevraagd worden om mee te doen (zij hebben eerder aangegeven dat ze voor aanvullend onderzoek benaderd mogen worden) .
Daarnaast doen ook de volgende cohorten mee: Amigo en Piama (IRAS Universiteit Utrecht), en de PROSPECT studie (UMC Utrecht). Verder ter info: MORGEN en PROSPECT vormen samen de Nederlandse bijdrage aan de Europese EPIC-studie en worden gezamenlijk aangeduid als EPIC-NL.
Meerdere cohorten in Nederland willen hun populatie vragen om aanvullende data te leveren over COVID-19 zoals bevraagd in de COVApp om deze te kunnen analyseren in relatie tot de vaak langdurig verzamelde medische en leefstijlgegevens gegevens die de cohorten hebben over hun deelnemers. Met dit onderzoek wil men meer kennis verkrijgen over COVID-19 en achterliggende factoren en de invloed van chronische ziekten.
Het aanleverende proces voor het RIVM is de MORGEN en DCS studie. Ook andere cohorten zullen hun deelnemers vragen mee te nemen aan dit onderzoek.
Er is nog geen gezamenlijk datamanagementplan opgesteld waardoor er nog geen overzicht is de afnemende processen en organisaties.

Context (systeemdecompositie)



Fase 2: IMPACT

Impact (QIS)

I	Samenvatting										
	STAP 1		STAP 2			STAP 3					
	Rubricering		Classificatie proces		Classificatie systeem		B		I		V
	Openbaar		Ondersteunend		Nuttig	X	Laag		Laag		Laag
	RIVM Intern (besloten)	X	Bijdragend		Belangrijk		Midden	X	Midden	X	Midden
	RIVM Vertrouwelijk		Strategisch	X	Vitaal		Hoog		Hoog		Hoog
	Departementaal Vertrouwelijk		Kritisch strategisch								
	Staatsgeheim Confidentieel										
	Staatsgeheim Geheim										
	Staatsgeheim Zeer Geheim										

Proces: Het proces is geclassificeerd als 'bijdragend'. De data en het onderzoek dat uit dit proces volgt kan bijdragen aan het krijgen van een beter inzicht in de impact van COVID-19 op de gezondheid en leefstijl.

Systeem: Het systeem is geclassificeerd als 'vitaal'. Het RIVM sluit zich aan bij een landelijk onderzoek binnen cohorten. Er zal geen alternatief worden gemaakt indien deze app niet goed werkt.

Informatie: De beschikbaarheid van CovApp is gesteld op 'midden'. De impact als er problemen zijn met de vertrouwelijkheid zullen groter zijn dan normaliter gezien het een Corona onderzoek betreft met bijzondere persoonsgegevens en de betrokkenheid van het RIVM hierin.

Fase 3: Dreigingen

(impact, kans en risico)

Dreigingen, impact en kans (organisatorisch)

Overzicht van de relevante dreigingen met daarbij de mogelijke impact (vanuit de actoren) in relatie tot de kans met uiteindelijk organisatorische maatregelen.

R #	Gebeurtenissen ('threat events')	Consequenties / impact	Impact	Kans	
R01	· Gebruik van de onrechtmatig verkregen inloggegevens van een medewerker of andere belanghebbende (brute-force aanval, phishing wachtwoord raden, onbeveiligde opslag van gegevens, gebruik van hetzelfde wachtwoord in meerdere, onafhankelijke omgevingen)	Onrechtmatig verkregen inloggegevens betreffen de deelnemer en de RIVM medewerker. De deelnemer gebruikt de app op de smartfoon of het webformulier. De RIVM gebruikt alleen direct toegang. Bij onrechtmatig verkregen inloggegevens van de deelnemer loopt deelnemer tijdens de invoersessie het risico dat iemand kan meekijken (1 deelnemer). Bij onrechtmatig verkregen inloggegevens van de RIVM medewerker kan dit meer deelnemers betreffen. Deelnemer ontvangt de inlogcode via een brief (post).	Midden	2	Laag
R02	· Misbruik van een kwetsbaarheid in het authenticatie en autorisatiemechanisme van een applicatie (bijvoorbeeld privilege escalation)	Onrechtmatig verkregen inloggegevens betreffen de deelnemer en de RIVM medewerker. De deelnemer gebruikt de app op de smartfoon of het webformulier. De RIVM gebruikt alleen direct toegang. Bij onrechtmatig verkregen inloggegevens van de deelnemer loopt deelnemer tijdens de invoersessie het risico dat iemand kan meekijken (1 deelnemer). Bij onrechtmatig verkregen inloggegevens van de RIVM medewerker kan dit meer deelnemers betreffen.	Midden	1	Zeer laag

Dreigingen, impact en kans (organisatorisch vervolg)

Overzicht van de relevante dreigingen met daarbij de mogelijke impact (vanuit de actoren) in relatie tot de kans met uiteindelijk organisatorische maatregelen.

R #	Gebeurtenissen ('threat events')	Consequenties / impact	Impact	Kans	
R03	- Session Hijacking (bijvoorbeeld session replay-aanvallen)	Onrechtmatig verkregen inloggegevens betreffen de deelnemer en de RIVM medewerker. De deelnemer gebruikt de app op de smartfoon of het webformulier. De RIVM gebruikt alleen direct toegang. Bij onrechtmatig verkregen inloggegevens van de deelnemer loopt deelnemer tijdens de invoersessie het risico dat iemand kan meekijken (1 deelnemer). Bij onrechtmatig verkregen inloggegevens van de RIVM medewerker kan dit meer deelnemers betreffen.	Laag	1	Zeer laag
R04	- Rechtstreeks misbruik van een kwetsbaarheid (ontbreken patch, misconfiguratie) in de infrastructuur (besturingssysteem, webserver, middleware, services, software)	Door ontbreken van een patch kan iemand toegang krijgen tot de gegevens van 1 of meer deelnemers.	Midden	1	Zeer laag
R05	- Diefstal (lezen)/fraude/lekken van (gevoelige) gegevens	Iemand kan toegang krijgen tot de gegevens van 1 of meer deelnemers.	Midden	2	Laag
R06	- Fraude door de invoer van valse transacties	Door valse transacties kan het systeem overbelast of in de war raken.	Laag	1	Zeer laag
R07	- Aanpassing van gegevens, manipulatie van programmatuur voor na ingebruikname	Het systeem werkt niet goed. Er is een risico dat iemand alle onderzoeksdata wijzigt. Of dat bij een vrij veld valse gegevens worden ingevoerd.	Midden	1	Zeer laag

Dreigingen, impact en kans (organisatorisch vervolg)

Overzicht van de relevante dreigingen met daarbij de mogelijke impact (vanuit de actoren) in relatie tot de kans met uiteindelijk organisatorische maatregelen.

R #	Gebeurtenissen ('threat events')	Consequenties / impact	Impact	Kans	
R08	· Vernietigen van gegevens	Gegevens zijn kwijt.	Laag	2	Laag
R09	· Installatie malware met als doel gegevens te vernietigen	Gegevens zijn kwijt.	Laag	1	Zeer laag
R10	· Installatie malware met als doel gegevens te lekken	Bij onopgemerkte installatie van malware op een smartfoon loopt deelnemer tijdens de invoersessie het risico dat iemand kan meekijken.	Midden	1	Zeer laag
R11	· Phishing (phishing, spear-phishing, whaling)	Als een deelnemer gebruik maakt van het webformulier dan kan d.m.v. fishing deelnemer naar een verkeerde website worden gestuurd.	Laag	1	Zeer laag
R12	· Ziektegolf door besmetting met virus of bacterie	Er is onvoldoende beheer van de website.	Midden	3	Middel

Fase 4: WEERBAARHEID

Weerbaarheid - risicobehandeling

In de volgende tabel zijn de mogelijke maatregelen weergegeven. Tevens is het restrisico weergegeven na implementatie van de maatregelen en eventuele aanvullende maatregelen.

R #	Gebeurtenissen ('threat events')	Maatregel	Restrisico
R12	Ziektegolf door besmetting met virus of bacterie	Regel vervanging van personeel bij RIVM en bij YourResearch.	

Bijlagen

Deelnemers risicoanalyse per fase

Deze risicoanalyse is uitgevoerd in januari 2021 en begeleid door 5.1.2e.
In onderstaande overzichten staan de deelnemers en de processtappen benoemd.

Fase	5.1.2e Informatie-manager	5.1.2e Privacy coördinator DVP	5.1.2e Information Security Consultant Brunel	5.1.2e CISO
Context	X	X	X	
Impact		X	X	
Dreigingen		X	X	
Weerbaarheid				
Rapportage		X	X	X