Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

DR RIVM

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 5.1.2e
info@rivm.nl

memo

Risicoanalyse bestelproces COVID-19 vaccins

Datum
17 januari 2021

Ons kenmerk

Uw kenmerk

Behandeld door
5.1.2e

5.1.2e

Kopie aan

Bijlage(n)
1

Beste lezer,

Gevraagd besluit:
Er wordt gevraagd om:

(1) Akkoord te gaan met het accepteren van de zes groepen van informatie-beveiligings(rest)risico's (A t/m F) zoals deze nu bekend zijn (zie bijlage 'Aanvraagformulier risicoacceptatie bestelproces Covid-vaccins v0.6.docx') en in te stemmen met de voorgestelde acties. De risicoacceptatie loopt tot 1 februari 2021.

(2) Toestemming voor de start van het volgende deel van het bestelproces: bestellen door verpleeghuizen en huisartsenposten vanaf maandag 18 januari 2021, en;

(3) Toestemming van het gebruik van het Formdeskformulier voor bestellingen door externe partijen (ROAZ) vanaf 18 januari 2021.

Zie hieronder de conclusie en de samenvatting van de uitgevoerde risicoanalyse (d.d. 17 januari 2021). De risico-acceptatie en de oplegnotitie zijn besproken in een bestuurlijk overleg op DR-niveau RIVM op zondag 17 januari 2021. Hier is een apart verslag van gemaakt.

Analyse informatiebeveiligingsrisico's aanvraag- en bestelproces COVID-19 vaccins

Conclusie en advies: er zijn zes (rest)risicogroepen geïdentificeerd:

A. Dreiging statelijke actoren (BBN3 dreigingsniveau)
B. Tijdsdruk en ad hoc besluitvorming
C. Beveiligingsniveau SNPG Webapp
D. Beveiligingsniveau Formdeskformulier Covid-bestellingen
E. Beveiligingsniveau SAP-DVP en Winshuttle
F. Beveiligingsniveau Movianto

Hieronder vallen risico's die niet (geheel) gereed zijn of opgelost kunnen worden voor de start van het volgende deel van het bestelproces vanaf 18 januari 2021. Ook zijn er nog onbekende risico's die voort kunnen komen uit het verhoogde dreigingsniveau. Gezien het belang van de voortgang van de Covid-vaccinatiecampagne wordt geadviseerd om de volgende fase van het bestelproces desondanks in gang te zetten.

Achtergrond
De vaccinatiestrategie (wie gevaccineerd wordt, met welk vaccin en door welke partij) is voortdurend aan verandering onderhevig, maar wordt gaandeweg steeds duidelijker. Dit heeft invloed op de inrichting van het bestelproces. Op dit moment worden de vaccins al uitgeleverd aan de (25) GGD'en die personeel uit de acute zorg vaccineren. Vanaf maandag 18 januari 2021 kunnen de verpleeghuizen en huisartsenposten ook gaan bestellen via de SNPG Webapp. Ook wordt vanaf dat moment het Formdesk-formulier voor extern gebruik (door ROAZ) vrijgegeven.

Er zijn een drietal 'actoren' gedefinieerd die een rol spelen bij het daadwerkelijk misbruiken van de geïdentificeerde risico's/dreigingen.

Actor	**Mogelijk doel**
Statelijke actoren	Frustreren van de vaccindistributie om diverse redenen (afhankelijk van actor).
Hacktivisten	Frustreren van de vaccindistributie als vorm van protest.
Georganiseerde misdaad	Buitmaken van vaccins voor verkoop op de zwarte markt.

Doel en scope
Voorliggende risicoanalyse heeft een drieledig doel. Het eerste doel is om de reële dreigingen/risico's met betrekking tot informatiebeveiliging in kaart te brengen. Het tweede doel is om de kans op optreden van deze dreigingen zo klein mogelijk te maken door het nemen van mitigerende maatregelen. Het derde doel is het geïnformeerd besluiten over livegang van (delen van) het bestelproces, met inachtneming en acceptatie van restrisico's.

De scope van de risicoanalyse betreft de logistieke keten die binnen de invloedsfeer van het RIVM valt. Dit betreft het bestellen via de SNPG Webapp of via Formdesk, het doorzetten en verwerken van de bestelinformatie aan logistiek dienstverlener Movianto.

Het afleveren van de vaccins bij de bestellers/klanten valt buiten scope. Hiervoor is een apart proces ingericht via de werkgroepen beveiliging COVID-19 vaccinatiecampagne. DVP zet hierbij in op het zoveel mogelijk aansluiten bij richtlijnen en eisen die voortkomen uit farmaceutische wet- en regelgeving. Ook de inspectie (IGZ) en andere actoren (politie e.d.) zijn hierbij betrokken.

Aanpak
Deze risico-inventarisatie is gebaseerd op de risicoanalyses van het RIVM (conform ISO27005). Hiervoor zijn workshops "risicoanalyse" gehouden met betrokken interne partijen maar ook met leveranciers, softwareontwikkelaars en de vervoerder Movianto.

Voor het kwalificeren van de risico's zijn kleuren toegekend conform de gebruikte methode voor risicoanalyse waarbij rood aangeeft een (zeer)hoog risico, oranje en geel een middel risico aangeven en groen een (zeer)laag risico.

Een alternatieve werkwijze voor het bestelproces vanaf 18 januari 2021 is onderzocht, echter niet wenselijk. Invoering van deze werkwijze leidt tot een aanzienlijke vertraging (ca. 2 weken) van de start van de vaccinatiecampagnes en tot een onacceptabele toename van de werk- en foutenlast voor het LCC (DVP).

Voor het vervolg is belangrijk dat met spoed en urgentie doorgewerkt wordt aan het oplossen van de bevindingen, het duiden en in kaart brengen van alle (rest)risico's. Voorstel is hier een ervaren senior manager op te zetten. Deze is in beeld, maar moet nog gevraagd worden. Alle betrokkenen zijn van de urgentie doordrongen. Dit moet leiden tot een nieuwe (bestuurlijke) risico-acceptatie op DR-niveau op uiterlijk zondag 31 januari 2021.

Analyse van informatiebeveiligingsrisico's

De informatiebeveiligingsrisico's zijn op hoofdlijnen geïnventariseerd, waarbij de benodigde aanvullende maatregelen op BBN3/DepV nog uitgewerkt moeten worden.

De afgelopen weken zijn veel mitigerende maatregelen, pentesten uitgevoerd en acties afgerond, waardoor de bijbehorende risico's een lagere risicokwalificatie hebben gekregen en of opgelost zijn. Echter, er zijn nog zes (rest)risicogroepen geïdentificeerd. Hieronder vallen risico's die niet (geheel) gereed zijn of opgelost kunnen worden voor de start van het volgende deel van het bestelproces vanaf 18 januari 2021. Ook zijn er nog onbekende risico's die voort kunnen komen uit het verhoogde dreigingsniveau.

Een toelichting op de restrisico's is te vinden in het bijgevoegde acceptatieformulier.

Risicomatrix IB Risicoanalyse – eerste analyse

Risicomatrix					
kans / impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)		C E	B D F	A	
2 (midden)					
1 (laag)					

A: Dreiging statelijke actoren (BBN3 dreigingsniveau)
B: Tijdsdruk en ad hoc besluitvorming
C: Beveiligingsniveau SNPG webapp
D: Beveiligingsniveau Formdesk formulier COVID bestellingen
E: Beveiligingsniveau SAP DVP en Winshuttle
F: Beveiligingsniveau Movianto