Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
Ministerie van Volksgezondheid Welzijn & Sport

Programma Nederland Digitaal Veilig

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
17 december 2020

Ons kenmerk
3148890

nota

Advies nationale veiligheid inzake digitale ondersteuning bron en contactonderzoek van VWS

Algemeen

De afgelopen maanden hebben gezamenlijke expertsessies plaatsgevonden waarin NCSC en AIVD middels expertadviezen input hebben geleverd voor een dreigings- en risicoanalyse van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) t.a.v. digitaal bron- en contactonderzoek. De sessies zijn voortgekomen uit een eerder verzoek van VWS over advisering met betrekking tot nationale veiligheidsrisico's die gepaard gaan met de toepassing van digitale apps ter ondersteuning van de bestrijding van de COVID-19 crisis[1]. Het doorlopen risicoanalyseproces t.a.v. de digitale bron- en contactonderzoek (dbco) app is vergelijkbaar met het doorlopen proces bij CoronaMelder. Ten aanzien van de CoronaMelder zijn veiligheidsadviezen uitgebracht d.d. 8 juli 2020 en 14 augustus 2020[2].

Het resultaat van deze gezamenlijke sessies is door VWS verwerkt in het opgestelde rapport getiteld 'Dreigings- en risicoanalyse oplossing 2 -dbco app' (hierna: het Rapport). NCTV, NCSC en AIVD willen met deze nota hun waardering uitspreken voor de openheid en de ontvankelijkheid van VWS voor onze adviezen in dit proces. NCSC en AIVD onderschrijven de inhoud van het Rapport als zijnde een weergave van hetgeen besproken is in de expertsessies. Dit laat onverlet dat NCTV, NCSC en AIVD middels dit advies nog enkele aandachtspunten en overwegingen aan VWS willen meegeven rond de verdere ontwikkeling van de dbco app en het implementeren van de adviezen uit het Rapport.

Dit advies is net als het Rapport gebaseerd op de stand van zaken van de ontwikkeling van de app ten tijde van de sessies en op basis van de daarvoor van VWS ontvangen documentatie en de toelichting die in de sessies is gegeven. Het advies is gebaseerd op expertsessies en de daarin of in relatie tot die sessies aan ons beschikbaar gestelde informatie en inzichten. Dit advies is tevens gebaseerd op een aantal door VWS aangegeven (ontwerp) keuzes (zoals centrale opslag van gegevens).

[1] Zoals opgenomen in "Opdracht en samenstelling Waarborgen Nationale Veiligheid" d.d. 24 juni 2020.
[2] Tussenadvies d.d. 8 juli 2020, kenmerk 2966502; aanvullend advies d.d. 14 augustus, kenmerk 3002061.

Programma Nederland Digitaal Veilig

Datum
17 december 2020

Ons kenmerk
3148890

Proces

De ontwikkeling van een app is een dynamisch en iteratief proces waardoor dit advies nadrukkelijk gebaseerd is op de huidige inzichten en de stand van zaken ten tijde van de expertsessies. Een aantal (ontwerp)keuzes door VWS die op een later moment zullen worden gemaakt of mogelijk worden aangepast, bijvoorbeeld door middel van updates of andersoortige veranderingen op het gebied van deze app, kunnen nog leiden tot aanpassing van de risicoanalyse en daarmee ook tot aanpassing van dit advies m.b.t. benodigde additionele maatregelen.

Dit advies is dus niet te beschouwen als een alomvattend advies over de mogelijke cyber– en nationale veiligheidsrisico's. De uiteindelijke afweging van de te beschermen belangen en het beheersen van de risico's is een verantwoordelijkheid van het ministerie van VWS.

Adviezen

Op basis van het hierboven beschreven proces worden in dit hoofdstuk enkele adviezen gegeven op het gebied van de nationale veiligheid en cybersecurity in relatie tot de ontwikkeling van de dbco app.

Wanneer er significante keuzes worden gemaakt of veranderingen worden doorgevoerd in de architectuur zal het risicoanalyseproces opnieuw (gedeeltelijk) doorlopen moeten worden om te bezien of de dreigingen en risico's anders gewaardeerd dienen te worden.

De algemene beveiligingsadviezen[3] zoals gegeven bij CoronaMelder gelden ook voor deze dbco app. In dit advies zullen wij deze niet opnieuw herhalen, maar adviseren wij wel deze ook t.a.v. de dbco app in ogenschouw te nemen.

Scope

De belangrijkste verschillen tussen CoronaMelder en de dbco app zijn:

1. Het type en de omvang van de te verwerken gegevens.
2. De ketenafhankelijkheid waar het gaat om de samenwerking met de GGD'en.

Ten aanzien van het tweede punt is het essentieel om stil te staan bij de scope van de door VWS uitgevoerde risicoanalyse. De verwerking van de gegevens uit de dbco app vindt plaats binnen een keten met o.a. de GGD'en. De door VWS uitgevoerde risicoanalyse heeft slechts betrekking op het deel van de infrastructuur waar VWS verantwoordelijk voor is.

Om de veiligheid van de gegevens uit de dbco app te kunnen waarborgen moet de digitale weerbaarheid over de gehele keten op voldoende niveau zijn. In het bijzonder omdat de omvang van de te verwerken persoonsgegevens in de dbco app aanzienlijk groter is dan in de CoronaMelder app. Over de elementen die buiten de scope van de risicoanalyse van VWS vielen, zoals de huidige infrastructuur en de processen bij de GGD'en, kan thans geen advies afgegeven worden. In dit licht wordt geadviseerd andere ketenpartners, waaronder de

[3] Tussenadvies d.d. 8 juli 2020, kenmerk 2966502; aanvullend advies d.d. 14 augustus, kenmerk 3002061.

Programma Nederland
Digitaal Veilig

Datum
17 december 2020

Ons kenmerk
3148890

GGD'en, te betrekken bij de verdere risicoanalyse en het waarborgen van de digitale weerbaarheid.

VWS heeft de tijdens de workshops gegeven adviezen van AIVD en NCSC verwerkt in het Rapport. Deze adviezen worden daarom niet herhaald in deze brief. Dit advies gaat primair in op de ketenafhankelijkheden.

Werk intensief samen met de ketenpartners om de digitale weerbaarheid binnen de gehele keten te waarborgen
Wat betreft de digitale weerbaarheid hebben, binnen het dbco proces, verschillende organisaties verschillende verantwoordelijkheden. De risico's die zijn geïdentificeerd tijdens de risicoanalyse kunnen echter alleen beheerst worden indien er binnen de keten intensief wordt samengewerkt aan de risicobewustheid, de digitale weerbaarheid en de onderlinge afhankelijkheden in ogenschouw worden genomen.

Hieronder worden enkele voorbeelden gegeven van de gebieden waarop intensieve samenwerking en afstemming tussen de ketenpartners naar onze mening essentieel is voor het beheersen van de door VWS geïdentificeerde risico's:

1. Vergelijk de risicoanalyses met elkaar om te komen tot een ketenbreed risicobeeld te krijgen.
2. Stem de hieruit voortkomende security architectuur op elkaar af.
3. Richt een herhaaldelijk risicoanalyse proces in, wetende dat er wijzigingen in de dreiging en de IT infrastructuur zullen plaatsvinden.
4. Voer gezamenlijke oefeningen uit om de digitale weerbaarheid in de praktijk te toetsen.
5. Richt een gezamenlijk proces in waar het gaat om incident afhandeling en het beheersen van crisissituaties en stem hierin de verantwoordelijkheden en mandaten vooraf af.

Vergelijk de risicoanalyses met elkaar om te komen tot een ketenbreed risicobeeld
Omdat VWS en de ketenpartners slechts een deel van de keten overzien, is het belangrijk om de uitkomsten van de verschillende risicoanalyses met elkaar te vergelijken en hier conclusies aan te verbinden. Alleen door een ketenbreed risicobeeld te creëren kunnen er ketenbrede maatregelen worden getroffen die op elkaar zijn afgestemd. Daarnaast is dit ketenbrede risicobeeld het fundament onder effectieve samenwerking tussen de ketenpartners waar het gaat om het realiseren van de digitale weerbaarheid.

Concreet: Vergelijk de door de individuele ketenpartners opgestelde risicoanalyses met elkaar en stel ten aanzien van de risico's hierin de parallellen en delta's vast. Bepaal vervolgens of er ketenbrede risico's bestaan die nog niet in de risicoanalyses van de individuele ketenpartners zijn opgenomen.

Stem de hieruit voortkomende security architectuur op elkaar af
Aan de hand van het ketenbrede risicobeeld kan worden bepaald op welke punten de geïdentificeerde risico's gezamenlijk dienen te worden beheerst en waar

samenwerking en afstemming noodzakelijk zijn. Het gaat hierbij om zowel technische, procedurele, preventieve als detectieve maatregelen.

Deze security architectuur gaat verder dan slechts de beveiliging van de technische interfaces die de gegevensoverdracht mogelijk maken. De ketenpartners zullen naast de invulling van de preventieve maatregelen ook moeten nadenken over ketenbrede detectieve maatregelen en zaken zoals logging en forensic readiness met het oog op incident response.

Richt een herhaaldelijk risicoanalyse proces in, wetende dat er wijzigingen in de dreiging en de IT infrastructuur zullen plaatsvinden
Tijdens de levenscycli van de dbco infrastructuur zullen er veranderingen ontstaan aan zowel de kant van de dreiging als in de dbco infrastructuur. Deze veranderingen brengen mogelijk nieuwe risico's met zich mee of maken eerder hoog geprioriteerde risico's juist minder relevant. Dit maakt periodieke afstemming tussen de ketenpartners essentieel. Alleen met deze periodieke afstemming over het actuele ketenbrede risicobeeld kunnen de noodzakelijke aanpassingen worden gemaakt aan de maatregelenset.

Voer gezamenlijk testen en oefeningen uit om de digitale weerbaarheid in de praktijk te toetsen
Om het gewenste niveau van digitale weerbaarheid te garanderen, is het noodzakelijk om de technische maatregelen in de IT infrastructuur in de praktijk te toetsen. Dit kan onder andere aan de hand van redteaming (purpleteaming) oefeningen en penetratietesten. Omdat een aanvaller geen rekening houdt met wie voor welk deel van de keten verantwoordelijk is (deze neemt over het algemeen de weg van de minste weerstand om zijn doelen te bereiken) is ons advies om dergelijke testen ook gezamenlijk uit te (laten) voeren. Zo wordt de digitale weerstand van de keten met al haar afhankelijkheden als geheel getest en wordt duidelijk waar in de keten de eventuele zwakke plekken zitten.

Wetende dat niet alle risico's te beheersen zijn, is naast het testen van de technische maatregelen, het ook noodzakelijk om de afhandeling van incidenten en het omgaan met crisissituaties met elkaar te oefenen. Bij dergelijke oefeningen gaat het onder andere om het helder krijgen van procedures, mandaten en de beschikbaarheid van stakeholders.

Richt een gezamenlijk proces in waar het gaat om het afhandelen van incidenten en crisissituaties
Restrisico's maken het noodzakelijk om de keten voor te bereiden op onvermijdelijke incidenten en mogelijke crisissituaties. Hierbij is ons advies om vooraf afspraken te maken over o.a.:

- de te doorlopen processen/procedures bij incidenten en crisissituaties;
- de verschillende verantwoordelijkheden en mandaten tussen de ketenpartners;
- bereikbaarheid en (veilige) communicatie;
- vastlegging van informatie (logging) om de afhandeling van incidenten en crisissituaties te faciliteren,

en ervoor te zorgen dat eenieder die hierbij betrokken is, ook op de hoogte is van deze processen en deze op een eenduidige wijze worden aangeleerd.

Programma Nederland
Digitaal Veilig

Datum
17 december 2020

Ons kenmerk
3148890

Zoals eerder aangegeven, is ons advies om incidentafhandeling en crisissituaties ook als keten gezamenlijk te oefenen.

Conclusie

Op basis van de op dit moment beschikbare informatie over de dbco app en de inrichting daarvan, wordt – als de hierboven gegeven adviezen worden geïmplementeerd – weerbaarheid georganiseerd tegen potentiële risico's op het gebied van nationale veiligheid. In bovengenoemde adviezen komt nadrukkelijk het belang van het betrekken van en de samenwerking met ketenpartners naar voren. De geïnventariseerde risico's en mogelijke maatregelen kunnen daarom meegenomen worden in de afwegingen die VWS zal maken bij het implementeren van de dbco app. Dit laat onverlet dat dit beeld dient te worden bijgesteld zodra VWS nadere keuzes maakt m.b.t. de inrichting of andere informatie beschikbaar komt, en dat de dreiging en daaraan verbonden risico's na verloop van tijd kunnen veranderen.