Rijndijk 235
2394 CD Hazerswoude
Tel. (071) 3416911
Email noordbeek@noordbeek.com

Ministerie van Volksgezondheid, Welzijn en Sport

ISAE 4401 Rapport van feitelijke bevindingen over

Informatiebeveiliging en Privacybescherming

Aangaande een assessment

Van de Backend-omgeving van de CoronaMelder (de 'notificatie app')

Definitieve versie: 1.00

Opdrachtgever	B. de Winter	Ministerie van VWS
Auteur	R. Paans	Noordbeek B.V.
	S.D. Kubacki	
	J. Winkel	
Rapportnummer	VWSCOR0-1	
Classificatie	Openbaar	
Status	Definitief	
Datum	8 december 2020	
Bestandsnaam	Noordbeek Rapport Assessment Backend CoronaMelder 2020	

KvK nummer	Rijnland 33265070
BTW nummer	NL8203.45.180.B01

Colofon

Opdrachtgever	B. de Winter Chief Security & Privacy Operations (CSPO) Programma Realisatie Digitale Ondersteuning Ministerie van VWS
Opdrachtnemer	Prof.dr.ir. R. Paans RE Directeur Noordbeek B.V.
Contactpersoon	S.D. Kubacki Senior IT-auditor
Auteurs	S.D. Kubacki, Senior IT-auditor J. Winkel, Technical IT-auditor
Kwaliteitscontrole	W.H. Mulder, QA Officer Noordbeek B.V.

Inhoud

1. Inleiding

Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) laat de CoronaMelder ontwikkelen. Dit is de 'notificatie app'. Als onderdeel van het ontwikkel- en implementatieproces wordt een Backend-omgeving ingericht door het Agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), als uitvoeringsorganisatie van het ministerie van VWS, en KPN.

Het ministerie van VWS heeft Noordbeek opdracht gegeven een assessment uit te voeren op de beheersingsmaatregelen binnen de Backend-omgeving, gericht op informatiebeveiliging en privacybescherming.

Een assessment levert een beperkte mate van zekerheid, en is gericht op specifieke vragen die zijn geformuleerd door de opdrachtgever. Noordbeek levert de rapportage in de vorm van de International Standard on Assurance Engagements 4401 (ISAE 4401), met de Nederlandstalige naam 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden'.

De opdracht aan Noordbeek is onderdeel van een reeks aan onderzoeken en audits op de CoronaMelder, gericht op transparantie naar de burger en de volksvertegenwoordiging. In dit kader is dit ISAE 4401-rapport bedoeld om publiekelijk te worden gedeeld.

2. Rapport van feitelijke bevindingen met betrekking tot de assessment

Aan: Opdrachtgever

2.1. Opdracht

Wij hebben overeengekomen specifieke werkzaamheden verricht met betrekking tot een assessment op de beheersingsmaatregelen binnen de Backend-omgeving, gericht op informatiebeveiliging en privacybescherming.

De opdracht voor de assessment is overeengekomen met het ministerie van VWS en heeft als doel een beperkte mate van zekerheid te bieden dat de vereiste beheersingsmaatregelen in opzet en bestaan aanwezig zijn, en eventuele afwijkingen te beschrijven. Hierbij worden de getroffen beheersingsmaatregelen getoetst tegen de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems – Requirements', de NIB-richtlijn en de Cyber Security Act normering.

De overeengekomen specifieke werkzaamheden zijn tot stand gekomen in overleg met de beoogde gebruikers, zijnde het ministerie van VWS, CIBG en KPN.

De opdrachtvoorwaarden zijn omschreven in onze opdrachtbrief van 10 augustus 2020, uitgebracht door Vanberkel Professionals B.V., mede namens Noordbeek B.V.

De rapportage wordt publiekelijk beschikbaar gesteld. Het onderzoek dient op een reproduceerbare wijze te worden beschreven, zodat publieke verificatie mogelijk is.

2.2. Verantwoordelijkheden

Het is de verantwoordelijkheid van het ministerie van VWS om te bepalen of de overeengekomen specifieke werkzaamheden toereikend en geschikt zijn voor het hierboven beschreven doel.

Wij hebben onze werkzaamheden verricht in overeenstemming met de Nederlandse Standaard 4401 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden' van de Nederlandse Orde van Register IT-Auditors (NOREA).

Bij het uitvoeren van deze opdracht hebben wij ons gehouden aan de voor ons geldende relevante ethische voorschriften in de Verordening Gedrags- en Beroepsregels Accountants (VGBA). Verder hebben wij de onafhankelijkheidsregels van de Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten (ViO) in acht genomen.

2.3. Werkzaamheden en bevindingen

In aanvulling op de uitleg van de randvoorwaarden van de opdracht, zoals vermeld in de paragraaf 'Opdracht' is in deze paragraaf een beschrijving van de overeengekomen specifieke werkzaamheden en feitelijke bevindingen opgenomen.

Wij doen geen uitspraak over wat de feitelijke bevindingen betekenen voor informatiebeveiliging en privacybescherming binnen de Backend-omgeving van de CoronaMelder in zijn totaliteit. Het ministerie van VWS, CIBG en KPN zullen hierover een eigen afweging moeten maken waarbij het ministerie van VWS, CIBG en KPN gebruik kunnen maken van dit rapport van feitelijke bevindingen en eventuele andere beschikbare informatie.

Conform de opdracht in de offerteaanvraag zijn wij bij deze assessment nagegaan of er een redelijke mate van zekerheid kan worden verkregen met betrekking tot de volgende punten:

1. Het hebben genomen van relevante beveiligingsmaatregelen in het datacenter, die zich verhouden tot de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems – Requirements'. Deze standaard komt qua normatiek overeen met de Baseline Informatiebeveiliging Overheid (BIO) op Basis Beveiligingsniveau (BBN) 2;
2. Verificatie van de instellingen conform de gemaakte afspraken en beloftes in de Data Protection Impact Analyse (DPIA);
3. Inventarisatie van de aanwezige certificering, validatie van de certificaten;
4. Beschikbaarheid van relevante DPIA's rond het datacenter en het beheersbaar hebben van de privacyrisico's;
5. Voldoen aan de NIB-richtlijn en de Cyber Security Act normering (voor zover van toepassing).

In overeenstemming met de opdrachtvoorwaarden zijn wij nagegaan of:

- De vereiste beheersingsmaatregelen voor informatiebeveiliging en privacybescherming in de Backend-omgeving van de CoronaMelder binnen CIBG en KPN zijn gedocumenteerd ('opzet');
- Deze maatregelen daadwerkelijk zijn getroffen ('bestaan');
- Deze maatregelen voldoen aan de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems – Requirements', de NIB-richtlijn en de Cyber Security Act normering.

Wij hebben geen onderzoek gedaan naar de operationele effectiviteit ('werking') van de beheersingsmaatregelen.

De bevindingen vanuit onze werkzaamheden en de daaruit voortvloeiende adviezen zijn als volgt:

1. **Fysieke beveiliging en BBN3** (zie 3.4.3)
   Het ministerie van VWS heeft (te) beperkte eisen geformuleerd voor het inrichten van de fysieke beveiliging van de datacenters. Dit heeft geleid tot een inrichting op Basisbeveiligingsniveau 2 (BBN2), conform de Baseline Informatiebeveiliging Overheid (BIO). BBN2 is bedoeld voor reguliere risico's.
   Naar onze mening is er sprake van een verhoogd risico voor de privacybescherming van de burgers met de CoronaMelder app en voor het imago van de staat, en moet rekening worden gehouden met dreigingen zoals statelijke actoren, beroepscriminelen, activisten etc. Daarvoor geldt het hogere Basisbeveiligingsniveau 3 (BBN3) en dienen aanvullende beveiligingsmaatregelen te worden getroffen conform het Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie (VIR-BI).
   Wij adviseren het ministerie van VWS een risicoanalyse uit te voeren om vast te stellen of sprake moet zijn van BBN2 of BBN3, en in het geval van BBN3 de daartoe vereiste aanvullende beveiligingsmaatregelen overeen te komen met CIBG en KPN.
   Tevens adviseren wij het ministerie van VWS niet te volstaan met onze huidige beperkte steekproef binnen deze assessment, maar een volledige audit te laten uitvoeren op de fysieke beveiliging en de fysieke inrichting van de Backend-omgeving;

2. **Accountbeheer voor beheeraccounts en systeemaccounts** (zie 3.3.1 / 3 / 4)
   Bij onze analyse van het accountbeheer voor de reeds ingerichte beheeraccounts en systeemaccounts hebben wij geen risico's gesignaleerd voor informatiebeveiliging. Wij missen echter een geaccordeerd overzicht van alle accounts in de Backend-omgeving, met een toelichting waarvoor deze zijn bedoeld en welke specifieke instellingen daarbij nodig zijn. Tevens hebben wij geconstateerd dat de relevante omgevingen ten tijde van ons onderzoek nog werden opgebouwd, waardoor geen volledige oordeelsvorming mogelijk was.
   Wij adviseren CIBG een overzicht op te stellen van alle accounts in de Backend-omgeving met een toelichting en een specificatie van hun instellingen, en een proces in te regelen om dit overzicht actueel te houden en wijzigingen te laten accorderen door de Chief Security & Privacy Operations (CSPO), Programma Realisatie Digitale Ondersteuning.

2.4. Overzicht van de adviezen

De in dit rapport opgenomen adviezen zijn hieronder samengevat. Wij maken in de kolom 'Prioriteit' onderscheid tussen al lopend, korte termijn (binnen 6 maanden), middellange termijn (tussen 6 en 12 maanden) en lange termijn.

Sectie	Advies	Prioriteit
3.3.1 3.3.3 3.3.4	**Accountbeheer voor beheeraccounts en systeemaccounts** Wij adviseren CIBG een overzicht op te stellen van alle accounts in de Backend-omgeving met een toelichting en een specificatie van hun instellingen, en een proces in te regelen om dit overzicht actueel te houden en wijzigingen te laten accorderen door de CSPO, Programma Realisatie Digitale Ondersteuning.	Korte termijn
3.4.3	**Fysieke beveiliging, besluit over BBN2 versus BBN3** Wij adviseren het ministerie van VWS een risicoanalyse uit te voeren om vast te stellen of sprake moet zijn van Basisbeveiligingsniveau 2 (BBN2) of Basisbeveiligingsniveau 3 (BBN3), en in het geval van BBN3 de daartoe vereiste aanvullende beveiligingsmaatregelen overeen te komen met CIBG en KPN.	Lopend
3.4.3	**Fysieke beveiliging, volledige audit** Wij adviseren het ministerie van VWS niet te volstaan met onze huidige beperkte steekproef op de inrichting van de datacenters binnen deze assessment, maar een volledige audit te laten uitvoeren op de fysieke beveiliging en de fysieke inrichting van de Backend-omgeving.	Korte termijn
-	**Volledige audit op de operationele Backend-omgeving** Wij adviseren de in dit rapport beschreven assessment op de opzet en bestaan van de Backend-omgeving en -processen in opbouw, te laten volgen door een volledige audit op het moment dat de omgeving en processen operationeel zijn. Dit dient een audit op opzet en werking te zijn. Hierbij wordt de operationele effectiviteit van de getroffen beheersmaatregelen getoetst.	Korte termijn

2.5. Vrij gebruik van het rapport en de verspreidingskring

Bij het opstellen van deze rapportage is rekening gehouden met de verwachtingen van de beoogde gebruikers, namelijk de burgers en de volksvertegenwoordiging, en de eis van de opdrachtgever dat publieke verificatie mogelijk moet zijn. Daarom is deze rapportage zo opgezet dat deze publiekelijk kan worden gedeeld.

Hazerswoude, 8 december 2020

Prof.dr.ir. R. Paans RE
Directeur Noordbeek B.V.

3. Detailrapport: Waarnemingen en conclusies per aandachtsgebied

Wij hebben de in bijlage A genoemde functionarissen geïnterviewd of gesproken, en de in bijlage B genoemde documenten bestudeerd.

Wij hebben waarnemingen voor de fysieke beveiliging uitgevoerd op de locatie 'KPN Datacenter AM8 zone 1' en voor de HSM sleutelceremonie bij Justid en CIBG. Onze waarnemingen en conclusies zijn hieronder per aandachtsgebied uitgewerkt.

Het door ons ontwikkelde werkprogramma voor het inventariseren van de beheersingsmaatregelen in relatie tot de eisen voor informatiebeveiliging en privacybescherming is gericht op het verkrijgen van de mate van inzicht dat nodig is voor het leveren van publieke transparantie. De aanpak en het werkprogramma zijn voorafgaand aan het onderzoek afgestemd met de opdrachtgever. De bevindingen zijn in concept afgestemd met CIBG en KPN.

In de onderstaande tekst refereren wij aan de documentatie in de vorm van '[doc x.x.y]', waarbij 'x.x' het nummer van de getoetste beheersingsmaatregel in ons werkprogramma is, en 'y' een volgnummer in de vorm van een letter. Indien een document relevant is voor meerdere beheersingsmaatregelen, hebben wij voor het nummer 'x.x' de meest relevante maatregel gekozen.

3.1. De IT-omgeving

3.1.1. Beschrijving IT-omgeving

Norm 1.1 is: *De huidige IT-omgeving is in voldoende mate beschreven*.

Wij hebben de volgende documentatie ontvangen:

1.1.a	KPN, 'CoronaMelder App VWS – CIBG – High Level Design (HLD)', versie 0.29	23-07-2020
1.1.b	KPN, 'VWS – CIBG – CoronaMelder App Low Level Design (LLD)', versie 0.15	29-07-2020
1.1.c	KPN, 'High Level Design Beschrijving, Ministerie van VWS – CIBG, CoronaMelder App', versie 0.2	18-08-2020
1.1.d	CIBG, 'Corona App – Functioneel-Technisch Ontwerp', versie 0.7	14-08-2020
1.1.e	'Raamovereenkomst ARBIT-2016 tussen Ministerie van Volksgezondheid, Welzijn en Sport, CIBG, IGZ en ESIT, en KPN B.V. inzake Managed Hosting & Storage services met kenmerk 201700274.068'	23-05-2017

De verantwoordelijkheden voor de Backend-omgeving zijn als volgt belegd:

- Het ministerie van VWS is verantwoordelijk voor de ontwikkeling van de software en het applicatie management. Deze aspecten vallen buiten de scope van ons onderzoek;
- CIBG is de leverancier van de middleware-laag op de hosting en de leverstraat voor autodeployments door middel van Azure Devops en Pipelines;
- KPN is de leverancier van de cloud-diensten tot en met de besturingssystemen, de firewalls en de load balancing. De Hardware Security Modules (HSM's) worden vanuit een colocatieoplossing aangesloten.

CIBG is de uitvoeringsorganisatie van het ministerie van VWS, met als doelstelling het bieden van transparante en betrouwbare data en informatie in zorg en welzijn. Organisaties, mensen en soms zelfs de gezondheid van mensen zijn hiervan afhankelijk. Meer informatie staat op https://www.cibg.nl/over-het-cibg.

KPN is de service provider voor Managed Hosting & Storage services, onder andere gericht op Cloud Services [doc 1.1.e]. Samen met CIBG ondersteunt KPN al andere dienstverlening voor het ministerie van VWS, zoals het Donorregister. De Backend-omgeving is hieraan toegevoegd.

De op te leveren Backend-omgeving is beschreven in het 'High Level Design (HLD)' [doc 1.1.a], het 'Low Level Design' [doc 1.1.b], de 'High Level Design Beschrijving' [doc 1.1.c] en het 'Functioneel-Technisch Ontwerp' [doc 1.1.d].

De conclusie is: *De Backend-omgeving voldoet aan norm 1.1, want de IT-omgeving is in voldoende mate beschreven. De verantwoordelijkheden van de betrokken partijen zijn eenduidig belegd en afgebakend*.

3.1.2. Applicaties en de toekomst

Norm 1.2 is: *Ontwikkelingen in de IT-omgeving in de nabije toekomst zijn bekend*.

In de 'High Level Design Beschrijving' [doc 1.1.c] is toegelicht dat de Backend-omgeving moet worden opgeleverd met (citaat): 'een extreem kort voortraject en een korte deadline'. Dit is ingevuld via Managed Hosting en een Cloud-oplossing.

Volgens het 'Programma van Eisen' [doc 1.3.a] is een belangrijke eis de schaalbaarheid. Dit is eis Q5: '*De server en gebruikte infrastructuur zijn eenvoudig op en af te schalen*'. Dit is gerealiseerd via de gekozen Cloud-oplossing. De verwachting is dat via de gekozen vorm van de inrichting de capaciteit op een flexibele wijze kan worden geleverd die nodig is voor een nationale uitrol van de CoronaMelder app.

Het proces voor het indienen en afhandelen van wijzigingen is beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a].

De conclusie is: *De Backend-omgeving voldoet aan norm 1.2, want er is een proces ingericht om de verwachte toekomstige ontwikkelingen af te handelen.*

3.1.3. Eisen en wensen

Norm 1.3 is: *De eisen en wensen voor de IT-omgeving zijn bekend*.

Wij hebben de volgende documentatie ontvangen:

1.3.a	'Programma van Eisen voor een digitale oplossing ter aanvulling op bron- en contactonderzoek', versie 0.5	19-05-2020
1.3.b	Kamerbrief bijlage, Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19, 'Advies 1: Programma van Eisen voor digitale oplossing ter aanvulling op bron- en contactonderzoek GGD', versie 0.4	16-07-2020

Het 'Programma van Eisen' [doc 1.3.a] bevat de volgende eisen voor de server (citaat):

- *F19: De server slaat tijdelijk contactcodes van besmette personen op na een positieve COVID-19-test;*
- *F20: De server verwijdert contactcodes automatisch na een vooraf ingestelde tijd;*
- *Q5: De server en gebruikte infrastructuur zijn eenvoudig op en af te schalen;*
- *Q7. Communicatie tussen de app en de server is gebaseerd op courante en bewezen standaarden;*
- *Q19. De app, de server en update faciliteit zijn voorbereid op het uitvallen van benodigde technologie en kan zonder foutmelding en in beperkte mate functioneren zolang die technologie niet beschikbaar is;*
- *Q21: De server kan na een verstoring de situatie (contactcodes van besmette gebruikers) van een bepaald moment van voor de verstoring herstellen. De maximale periode van verlies is vastgelegd in een SLA;*
- *Q25. De server en daarmee ondersteunde processen voldoen aan de AVG;*
- *Q31. De app en de server zijn getoetst middels een risicoanalyse, Privacy Impact Assessment (PIA) en een penetratietest en alle daardoor ontdekte kwetsbaarheden zijn opgelost of als risico geaccepteerd;*
- *Q36. De communicatie tussen de app en de server kan worden getest in een testomgeving.*

In de 'High Level Design Beschrijving' [doc 1.1.c] is de Sectie 'Eisen en Wensen' opgenomen. Hierin is vermeld (citaat):

- *Er is geen detaillijst van eisen aan de hosting gezien het extreem korte voortraject en korte deadline waarbinnen geleverd moet worden. Gaande het traject zijn enkele eisen bovengekomen (gespecificeerd in dit document) en ingevuld in de oplossing. Dit is echter een nog lopend proces.*
  Het platform en de architectuur is daarom opgebouwd in het gedachtengoed van de bestaande VGA-kavels welke onder een Europese Aanbesteding al aan CIBG worden geleverd. Daarbij wordt er uitgegaan van technologie en inrichting zoals bekend is binnen de bestaande kavels en wordt daar zo min mogelijk van afgeweken: standaardisatie en hergebruik van wat bekend is. Een harde eis is daarbij dat het bouwteam van de VGA-kavels ook de hosting van de Corona App omgeving invult. Privacy en security is het uitgangspunt.
  Daarbij dient het volgende te worden gerealiseerd:

- *Een T-platform voor de backend, bestaande uit portaal en functionaliteit waarvan de App gebruik maakt;*
- *Een geografisch redundant AP-platform voor de backend met een beschikbaarheid van 99,9%, bestaande uit portaal en functionaliteit waarvan de App gebruik maakt;*
- *Een koppeling met de CDN via welke mobiele keys worden uitgewisseld;*
- *Een koppeling met de API ten behoeve van de mobiele App;*
- *Ontsluiting van het portaal voor de GGD;*
- *Two-factor ontsluiting ten behoeve van beheer;*
- *Connectiviteit om door middel van Azure Pipelines deployments uit te voeren;*
- *Een oplossing ten behoeve van uitgifte van certificaten (PKIoverheid-certificaten);*
- *Colocatie voor een HSM-oplossing ten behoeve van keys voor de signing;*
- *Onderdelen ten behoeve van BIO-compliancy;*
- *Een oplossing t.b.v. Applicatie Logmanagement;*
- *Onderdelen ten behoeve van een SOC-SIEM-oplossing*.

Ten tijde van ons onderzoek was de ‘SOC-SIEM-oplossing’ buiten scope, aangezien die nog werd ingericht.

Waar mogelijk en waar relevant voor de Backend-omgeving hebben wij de bovenstaande eisen meegenomen tijdens ons onderzoek.

De conclusie is: De *Backend-omgeving voldoet aan norm 1.3, want de eisen en wensen zijn bekend*.

3.2. Besturing, Interne IT-beheersing en IT Governance

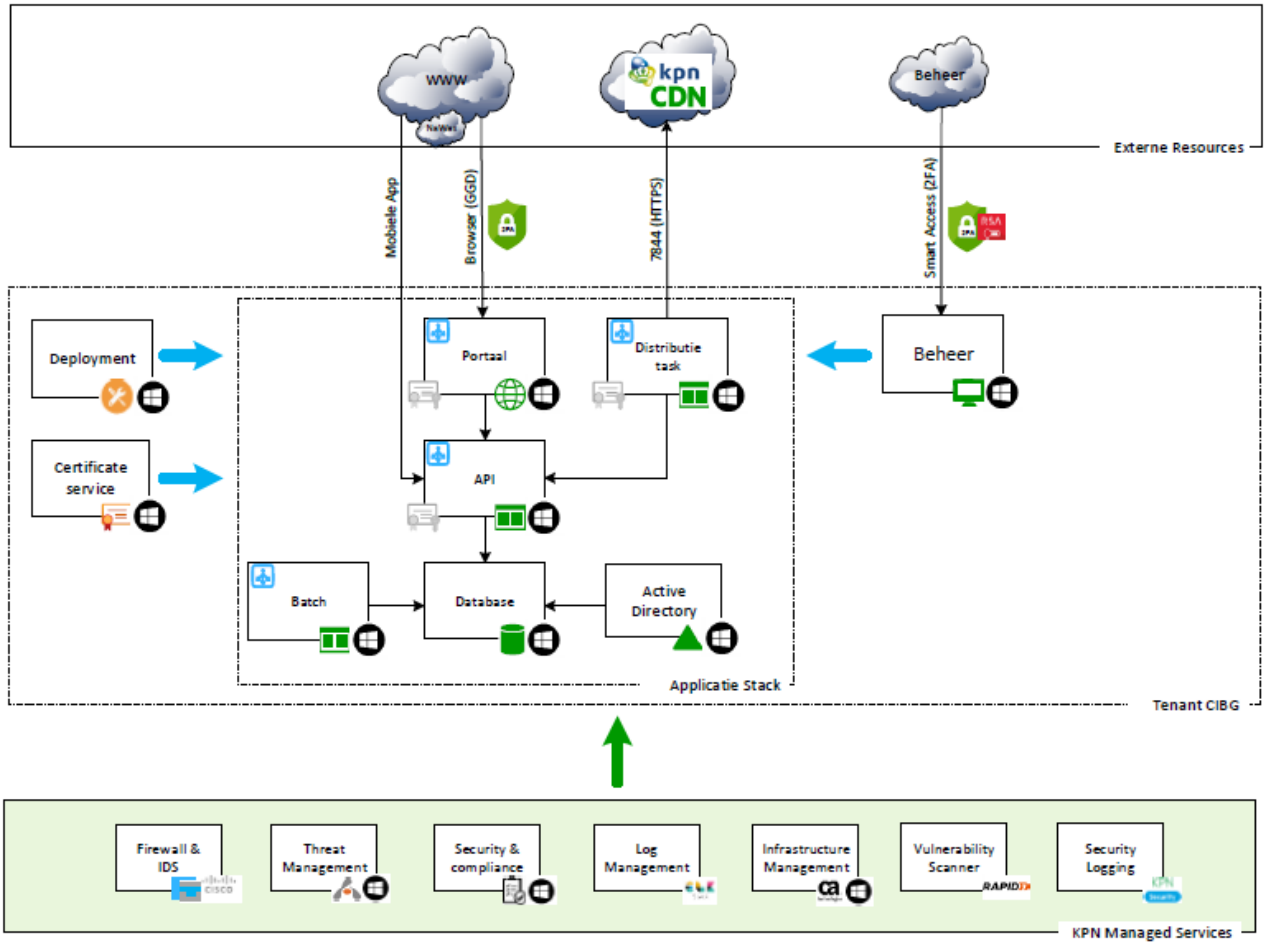
3.2.1. Strategie en beleid

Norm 2.1 is: *De IT-strategie is afgestemd op de actuele situatie van de organisatie. In het IT-beleid zijn concrete doelen en resultaten benoemd.*

Wij hebben de volgende documentatie ontvangen:

2.1.a	KPN, 'Dossier Afspraken en Procedures (DAP) CIBG (een agentschap van Ministerie VWS)', versie 1.7	04-02-2020

In de 'High Level Design Beschrijving' [doc 1.1.c] is de scope als volgt weergegeven in hoofdlijnen (citaat):



- *De bouwblokken in de Applicatie Stack van bovenstaande tekening worden voor test enkelvoudig en voor Acceptatie en Productie redundant uitgevoerd (daar waar loadbalancer icoontjes zijn opgenomen en v.w.b. Database en Active Directory) voor wat betreft de nieuwe CIBG-tenant/kavel. Deze bouwblokken worden geleverd vanuit een security frame-*

work op basis van BIO en in een separaat kavel worden opgebouwd achter een eigen dedicated firewallcluster. De omgeving is daarbij onafhankelijk ingericht van andere kavels die CIBG afneemt.
- *Voor het CDN wordt connectiviteit ingeregeld met de distributie task component middels certificaten.*
- *Voor de signing wordt gebruik gemaakt van een HSM, waarmee vanuit colocatie wordt gekoppeld met de distributie task component.*
- *Verdere connectiviteit welke onderdeel vormt van de oplossing bestaat uit een koppeling ten behoeve van de App met het API-bouwblok en ten behoeve van de GGD met het portaal.*

In de 'High Level Design Beschrijving' [doc 1.1.c] is de Sectie 'Ontwerpkeuzes' opgenomen. Hierin is vermeld (citaat):

- *De backend welke wordt geleverd bestaat uit specifieke onderdelen benodigd voor de applicatie en het portaal (webservers, API-servers, distributie task servers, batchservers, databaseservers en Active Directory), ondersteunende onderdelen voor deployments (middels Azure Devops met Pipelines), certificaat beheer (certificaten server t.b.v. het produceren van CSR's) en beheer toegang (beheer server met 2FA). De opbouw en keuze van deze onderdelen borduren voort op al geleverde functionaliteit aan CIBG voor andere kavels;*
- *De backend heeft een koppeling met het CDN, ontsluiting van het portaal voor de GGD en ontsluiting voor de App via de API-servers. Verder wordt er vanuit colocatie van een HSM-oplossing gebruik gemaakt door de backend vanuit de distributie task servers. Deze HSM-oplossing is een vereiste vanuit VWS;*
- *Er wordt een managed ELK Stack aangeboden ter ondersteuning van Applicatie Logmanagement door CIBG;*
- *Ondersteunende onderdelen op de backend onderdelen zijn firewalling ten behoeve van netwerk segmentatie en perimeter beveiliging, F5 loadbalancing voor SSL-terminatie en verdeling van het verkeer en diverse securitycomponenten om aan BIO-regelgeving te voldoen.*

De operationele aspecten van de samenwerking tussen CIBG en KPN zijn beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a].

De conclusie is: *De Backend-omgeving voldoet aan norm 2.1, want de aanpak is afgestemd op de actuele eisen en er zijn concrete doelen en resultaten benoemd.*

3.2.2. IT-organisatie en Control

Norm 2.2 is: *De organisatie bewaakt de uitvoering van de IT-strategie, het IT-beleid en de IT-procedures, en de voortgang van projecten.*

Wij hebben de volgende documentatie ontvangen:

2.2.a	Ministerie van VWS, Kamerbrief, 'Landelijke introductie CoronaMelder', kenmerk 1722926-208233-DICIO	16-07-2020
2.2.b	Ministerie van VWS, 'Statusslide minister', versie 15.25	06-07-2020
2.2.c	Ministerie van VWS, 'Statusslide minister', versie 15.00	09-07-2020
2.2.d	Ministerie van VWS, 'Statusslide minister', versie 18.30-2	13-07-2020
2.2.e	Ministerie van VWS, 'Dashboard minister', versie 17.30	20-07-2020
2.2.f	Ministerie van VWS, 'Dashboard minister', versie 22.00-2	03-08-2020
2.2.g	Stuurgroep agenda's VWS, CIBG en KPN, juli, augustus en september 2020	17-07-2020 04-09-2020
2.2.h	CIBG Offerte Hosting Coronamelder, definitief	06-08-2020
2.2.i	Bijlage I. Reactie offerte 20 augustus 2020	20-08-2020
2.2.j	Bijlage II. Monitoring proposal backend CoronaMelder	02-09-2020
2.2.k	Bijlage III. Referentiegids covid-19 HSM beheer, versie 0.5	27-08-2020
2.2.l	Bijlage IV. Inrichting infrastructuur Datacenters covid-19 HSM beheer, versie 1.1	26-08-2020
2.2.m	Ministerie van VWS, Brief Reactie CIBG inzake offerte 20 augustus 2020	07-09-2020
2.2.n	Verslag sessie COVID-19 app rol CIBG	15-07-2020

3.2.2.1. Rapportage aan de minister

Datgene wat in het dashboard voor de minister [doc 2.2.b t/m f] betrekking heeft op de Backend-omgeving hebben wij, waar relevant en mogelijk, getoetst aan de ontvangen documentatie. Daarbij zijn door ons geen afwijkingen geconstateerd.

3.2.2.2. Regieorganisatie vanuit het ministerie van VWS

De regieorganisatie vanuit het ministerie van VWS is aanwezig. Er zijn formele verantwoordelijkheden vastgelegd op bestuurlijk niveau. Dit is als volgt toegelicht tijdens het interview met de projectleider VWS (citaat):

- '*Er wordt gewerkt conform de initiële opdracht van CIBG* [doc 2.2.h];
- *Op voorhand is een stuurgroep ingericht met daarin VWS, CIBG en KPN, onder voorzitterschap van VWS, die wekelijks op vrijdag vergadert* [doc 2.2.g];
- *Alle betrokken managementlagen, inclusief escalatielijnen, zijn vooraf overeengekomen;*
- *Inzake de dagelijkse aansturing hebben de projectleiders van het CIBG, KNP en VWS specifiek dagelijks overleg (vaak meerdere malen) teneinde de aansturing, risico's en inhoudelijke zaken te beheersen;*
- *De projectleiders van CIBG en KPN zijn daarnaast dagelijks onderdeel van het overall programmateam van VWS door deelname in de dagstarten van 'Fundament & Raamwerk', opdat naast de 'eigen' opdracht zowel CIBG als KPN ook kennis hebben van aanpalende zaken die relevant kunnen zijn voor de effectieve uitvoering van de opdracht*'.

Aan ons zijn de bovengenoemde documenten [doc 2.2.g t/m n] overhandigd, als toelichting op de werkzaamheden van de regieorganisatie. Alleen de reguliere rapportages ontbreken, die ten tijde van ons onderzoek nog moesten worden ingeregeld.

Ten tijde van ons onderzoek waren er nog geen serieuze escalaties geweest. Alle issues konden via de projectorganisatie worden opgelost.

3.2.2.3. Samenwerking CIBG en KPN

Gezien de korte doorlooptijd is geen klassiek projectplan gemaakt, zoals bij een watervalproject. De projectvoering is gedaan op basis van agility. Het project is uitgevoerd door een gezamenlijk projectteam van CIBG en KPN. Drie belangrijke mijlpalen zijn benoemd voor het aansturen van het project.

Dagelijks is er een ‘dagstart’ en een ‘dag-update’.

De projectleider van CIBG zorgt voor de dagelijkse voortgangsrapportages. KPN zorgt voor een wekelijkse interne KPN-rapportage.

Naar de mening van de geïnterviewden verloopt de samenwerking tussen CIBG en KPN constructief en effectief.

De conclusie is: *De Backend-omgeving voldoet aan norm 2.2, want de uitvoering van de IT-strategie, het IT-beleid en de IT-procedures, en de voortgang van projecten worden bewaakt*.

3.2.3. Risicobeheersing

Norm 2.3 is: *De organisatie heeft de IT-risico's geanalyseerd en de mitigerende maatregelen vastgelegd.*

Wij hebben de volgende documentatie ontvangen:

2.3.a	Spreadsheet, 'FMEA CoronaMelder risicoinschatting' (geen vermelding van auteur of versie)	-
2.3.b	Github, 'Baseline for the Proof of Concept'	06-07-2020
2.3.c	Github, 'FMEA CoronaMelder'	23-09-2020

3.2.3.1. Maatregelen voor risicomitigatie

In de 'High Level Design Beschrijving' [doc 1.1.c] is de Sectie 'Eisen en Wensen' opgenomen. Hierin is over risico's en risicomitigatie onder andere vermeld (citaat):

- *Gezien de gevoeligheid en gebruik van de app onderhevig zal zijn aan hackers en aanvallen zijn een aantal specifieke eisen over security en capaciteit besproken. Onderdeel van de oplossing zijn daarbij:*
  - *Gebruik van PKI-overheid certificaten, aanmaken van CSR is daarbij voorbehouden aan KPN volgens eerder vastgelegde procedure via een aparte certificaten server;*
  - *Gebruik van HSM voor gegarandeerde signing;*
  - *IP-adressen dienen niet in logs voor te komen en 'aan de voorkant' te worden gestript. Dit vindt plaats door de x-forwarded headers standaard niet door te sturen en verkeer via firewall-NAT, loadbalancer-NAT te laten verlopen;*
  - *Beperking van het aantal requests vanuit 1 IP-adres binnen een vastgestelde tijdseenheid;*
  - *Beperking van het totaalaantal requests binnen een vastgestelde tijdseenheid;*
  - *Informatie (in breedste zin) retentie binnen het platform te maximaliseren op 14 dagen.*

De eis van 14 dagen in de laatste bullet is aangepast naar een retentieperiode van maximaal 7 dagen.

3.2.3.2. Risicoanalyses voor maatschappelijk transparantie

Wij hebben generieke documenten ontvangen over risico's, namelijk de spreadsheet 'FMEA CoronaMelder risicoinschatting' [doc 2.3.a] en op Github technische risico-afwegingen in het document 'Baseline 19ort he Proof of Concept' [doc 2.3.b] en de 'FMEA CoronaMelder' [doc 2.3.c].

De bouwteams bij CIBG en KPN hanteren een log voor Risks, Actions, Issues and Decisions (RAID) voor geconstateerde issues. KPN heeft tijdens de interviews de inhoud van deze log op het scherm getoond. De RAID-log is geclassificeerd als 'KPN Intern'.

De conclusie is: *De Backend-omgeving voldoet aan norm 2.3, want er is publiekelijk toegankelijke documentatie met risico-analyses.*

3.2.4. Informatiebeveiliging

Norm 2.4 is: *De organisatie voldoet aantoonbaar aan ISO/IEC 27001:2013, de NIB-richtlijn en de Cyber Security Act.*

Wij hebben de volgende documentatie ontvangen:

2.4.a	Ministerie van VWS, 'Compliancyrapport implementatie verplichte webeisen CoronaMelder', versie 1.1	16-07-2020
2.4.b	CIBG, 'Strategisch beleidsdocument informatieveiligheid', versie 1.0	12-11-2018
2.4.c	CIBG, 'CIBG SSD Requirements, Security Requirements binnen Secure Software Development', versie 2.8	08-11-2019
2.4.d	CIBG, 'Overzicht en Planning Security Rapportage voor CIBG over het jaar 2019'	14-11-2019
2.4.e	KPN Security, 'Maandelijkse security rapportage van de systemen van het CIBG over het eerste kwartaal 2020'	16-04-2020

Zowel CIBG als KPN beschikken over actuele beleidsdocumenten voor informatiebeveiliging. CIBG heeft haar 'Strategisch beleidsdocument informatieveiligheid' [doc 2.4.b] aan ons overlegd, en de KPN Security Policy (KSP) staat op de website van KPN. De gebruikte KPN datacenters beschikken over actuele certificaten voor compliance met ISO/IEC 27001:2013 'Information Security Management Systems Requirements' [doc 4.3.a t/m c].

CIBG volgt richtlijnen van NCSC en het Centrum voor Informatiebeveiliging en Privacy (CIP), zoals blijkt uit het document 'CIBG SSD Requirements, Security Requirements binnen Secure Software Development' [doc 2.4.c].

Een aantal operationele aspecten van informatiebeveiliging is beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a].

In de 'High Level Design Beschrijving' [doc 1.1.c] is de Sectie 'Security opties' opgenomen. Hierin is vermeld (citaat):

- *Aangezien de oplossing een oplossing voor de overheid betreft, is BIO-normering aan de orde. Daarbij worden de volgende managed onderdelen geleverd vanuit KPN Security:*
  - *Antivirus (McAfee);*
  - *Intrusion Detection en Protection (Cisco ASA);*
  - *Vulnerability scanning (Nessus of Qualys);*
  - *Compliancy scanning (Compas);*
  - *Log management (Qradar);*
  - *Pentesting (1x jaar);*
  - *Reporting (op bovenstaande onderdelen).*
- *Verder wordt een managed ELK Stack geleverd ten behoeve van applicatie log management;*
- *Uiteraard is de omgeving daarnaast beschermd tegen DDOS-aanvallen via de standaard NaWas dienst op het platform.*

KPN hanteert de Wet beveiliging netwerk- en informatiesystemen (Wbni) en de Telecommunicatiewet. KPN valt onder toezicht van Agentschap Telecom. Voor de Wbni doet KPN melding bij het NCSC wanneer de drempelwaarde hiertoe vereist.

KPN is bekend met de 'EU Richtlijn 2019-881 Cybersecurity Act' en adopteert elementen als onderdeel van het eigen KPN Security Policy (KSP) beleid.

CIBG en KPN bewaken de actuele informatiebeveiliging, zoals blijkt uit 'Overzicht en Planning Security Rapportage voor CIBG over het jaar 2019' [doc 2.4.d] en 'Maandelijkse security rapportage van de systemen van het CIBG over het eerste kwartaal 2020' [doc 2.4.e].

De conclusie is: *De Backend-omgeving voldoet aan norm 2.4, want er is aantoonbaar voldaan aan ISO/IEC 27001:2013, de NIB-richtlijn en de Cyber Security Act*.

3.2.5. Privacybescherming

Norm 2.5 is:

- *Persoonsgegevens worden adequaat behandeld en beschermd, conform doelbinding, proportionaliteit en subsidiariteit.*
- *De in de DPIA voorgestelde maatregelen zijn gerealiseerd.*

Wij hebben de volgende documentatie ontvangen:

2.5.a	Ministerie van VWS, Directie Informatiebeleid, CIO 'Gegevensbeschermingseffectbeoordeling (DPIA) COVID-19 notificatie-app', vastgesteld	07-07-2020
2.5.b	Ministerie van VWS, 'Privacy Governance 2018', versie 1.2	28-11-2018
2.5.c	Ministerie van VWS, 'Draaiboek Incidenten en Datalekken VWS', versie 1.1	23-01-2020
2.5.d	Ministerie van VWS, Panel van burgers, 'Ethische analyse van de COVID-19 notificatie app ter aanvulling op bron en contactonderzoek GGD'	14-07-2020

Voor privacybescherming valt CIBG onder het beleid van het ministerie van VWS. In dit kader hebben wij de documenten 'Privacy Governance 2018' [doc 2.5.b] en 'Draaiboek Incidenten en Datalekken VWS' [doc 2.5.c] ontvangen.

KPN heeft haar Privacy Reglement gepubliceerd op https://www.kpn.com/algemeen/missie-en-privacy-statement/privacy-statement.htm. Voor datalekken volgt KPN de vigerende wetgeving, inclusief meldingen bij de Autoriteit Persoonsgegevens.

Wij hebben de 'Gegevensbeschermingseffectbeoordeling (DPIA) COVID-19 notificatie-app' [doc 2.5.a] ontvangen. In de DPIA voorgestelde maatregelen die betrekking hebben op de Backend-omgeving hebben wij in andere onderdelen van dit rapport nagetrokken.

De conclusie is: *De Backend-omgeving voldoet aan norm 2.5, want persoonsgegevens worden adequaat behandeld en beschermd, conform doelbinding, proportionaliteit en subsidiariteit voor privacybescherming, en de in de DPIA voorgestelde maatregelen zijn gerealiseerd. Het woord 'adequaat' heeft hierbij betrekking op het proces, en staat los van eventuele bevindingen verderop in dit rapport met betrekking tot specifieke beheersingsmaatregelen.*

3.2.6. Opvolging van voorgaande audit aanbevelingen

Norm 2.6 is: *De aanbevelingen uit audits zijn opgevolgd of er zijn verbeterplannen*.

De Backend-omgeving is nog in opbouw. Er zijn geen voorgaande audit-rapporten over deze omgeving.

Wij hebben de DPIA ontvangen, welke is besproken in Sectie 3.2.5.

Wij hebben rapportages ontvangen vanuit de pentesten, die zijn besproken in Sectie 3.4.11. Via een steekproef op de interne communicatie tussen CIBG, KPN en de pentesters hebben wij vastgesteld dat verbeteracties worden uitgevoerd voor via de pentesten gesignaleerde zwakheden. Ten tijde van ons onderzoek liep nog een hertest voor een van de pentesten.

De bouwteams bij CIBG en KPN hanteren een log voor Risks, Actions, Issues and Decisions (RAID) voor geconstateerde issues. Wij hebben op het scherm kennis genomen van de inhoud van deze log, die doorlopend wordt geactualiseerd tijdens het inrichtingsproces.

De conclusie is: *De Backend-omgeving voldoet aan norm 2.6, want de aanbevelingen uit audits zijn opgevolgd of er zijn verbeterplannen*.

3.3. Accountbeheer en wachtwoordbeleid

3.3.1. Accountbeheer

Norm 3.1 is: *Accounts worden individueel toegekend. Er worden geen groepsaccounts gebruikt. Een overzicht van alle accounts is beschikbaar*.

Wij hebben de volgende documentatie ontvangen:

3.1.a	CIBG, 'Uitdraai 2020 03 CIBG Active Directory'	01-04-2020
3.1.b	Noordbeek, 'Analyserapport Active Directory COVP'	20-08-2020

In de Backend-omgeving wordt gebruik gemaakt van 1 generiek beheeraccount van KPN en individuele accounts van CIBG.

Wij hebben de uitdraai van de Active Directory (AD) van de Productie-omgeving geanalyseerd. De status van alle accounts op 20 augustus 2020 is:

- Er zijn 24 accounts in de Productie-omgeving, waarvan 4 zijn vergrendeld;
- Bij 2 vergrendelde accounts staat de vlag 'Password not required' (PASSWD_NOTREQD) aan. Wij adviseren deze vlag uit te zetten;
- Bij 3 actieve accounts en 2 vergrendelde accounts staat de vlag 'PasswordNeverExpires' aan;
- Bij 1 actief account staat de vlag 'CannotChangePassword' aan;
- Bij alle accounts staat in het veld 'LastLogonDate' een logindatum van minder dan 180 dagen geleden of ouder. Dit is correct;
- Bij 1 actief account en 4 vergrendelde accounts is geen data beschikbaar in het veld 'LastLogonDate'. Op deze accounts is nog nooit ingelogd;
- Bij alle accounts staat in het veld 'PasswordLastSet' een wachtwoordwijzigingsdatum van minder dan 90 dagen geleden. Dit is correct;
- Bij 2 vergrendelde accounts is geen data beschikbaar in het veld 'PasswordLastSet'. Op deze accounts is nog nooit een wachtwoord ingesteld.

De status van de administratoraccounts is op 20 augustus 2020:

- Er zijn 6 actieve en 1 vergrendeld administratoraccounts in de Productie-omgeving;
- Bij 1 actief administratoraccount staat 'true' in het veld 'PasswordNeverExpires'. Voor dit account verloopt het wachtwoord nooit;
- Bij 1 vergrendeld administratoraccount is geen data beschikbaar in het veld 'LastLogonDate'. Op dit account is nog nooit ingelogd.

Wij signaleren in de Productie-omgeving geen risico's voor informatiebeveiliging. Wij hebben ook de uitdraaien van de AD's van de Test- en Acceptatie-omgevingen geanalyseerd, met een identieke conclusie.

Wij missen echter een geaccordeerd overzicht van alle accounts in de Backend-omgeving, met een toelichting waarvoor deze zijn bedoeld en welke specifieke instellingen daarbij nodig zijn.

Wij adviseren CIBG een overzicht op te stellen van alle accounts in de Backend-omgeving met een toelichting en een specificatie van hun instellingen, en een proces in te regelen om dit overzicht actueel te houden en bij wijzigingen te laten accorderen door de CISO.

De conclusie is: *De Backend-omgeving voldoet deels aan norm 3.1, want accounts worden individueel toegekend en CIBG gebruikt geen groepsaccounts. Er is echter geen gedetailleerd overzicht van alle accounts beschikbaar, met een specificatie van hun instellingen.*

3.3.2. Instroom, Doorstroom en Uitstroom (IDU)

Norm 3.2 is: *Accounts worden tijdig aangemaakt, gemuteerd, geblokkeerd en verwijderd, conform de personele wijzigingen*.

Wij hebben de volgende documentatie ontvangen:

3.2.a	CIBG, ‘Autorisatiebeheer generieke tooling en infrastructuur’, versie 0.1	05-08-2020

CIBG heeft een formeel proces voor Instroom, Doorstroom en Uitstroom.

De Backend-omgeving is nog in een bouwfase. Op dit moment zijn de bouwteams nog actief. Na afronding van de bouwfase wordt deze omgeving opgenomen in het reguliere IDU-proces.

Gezien de bouwfase hebben wij geen steekproef kunnen uitvoeren op recente tickets in het servicedesk-systeem voor autorisatiewijzigingen.

De conclusie is: *Norm 3.2 is op dit moment niet van toepassing op de Backend-omgeving, aangezien deze nog wordt opgebouwd. Waarnemingen zijn pas in de toekomst mogelijk.*

3.3.3. Key-gebruikers- en administratoraccounts

Norm 3.3 is: *Key-users en administrators gebruiken sterke wachtwoorden of Two Factor Authentication*.

Bij de analyse in Sectie 3.3.1 hebben wij gesignaleerd dat een gedetailleerd overzicht ontbreekt van de accounts in de Backend-omgeving. Er zijn individuele accounts met de status administratoraccount.

Zoals is beschreven in Sectie 3.3.5, geldt voor alle accounts een strikte wachtwoordsyntax.

Zoals is beschreven in Sectie 3.3.6, is inloggen van buitenaf alleen mogelijk via Two Factor Authentication.

De conclusie is: *De Backend-omgeving voldoet deels aan norm 3.3, want key-users en administrators gebruiken sterke wachtwoorden of Two Factor Authentication, maar een gedetailleerd overzicht van alle accounts ontbreekt*.

3.3.4. Systeemaccounts

Norm 3.4 is: *Voor systeemaccounts is geborgd dat geen misbruik mogelijk is*.

Bij de analyse in Sectie 3.3.1 hebben wij gesignaleerd dat een gedetailleerd overzicht ontbreekt van de accounts in de Backend-omgeving. Er zijn individuele accounts die zijn ingesteld als systeemaccounts.

Zoals is beschreven in Sectie 3.3.5, geldt voor alle accounts een strikte wachtwoordsyntax.

Zoals is beschreven in Sectie 3.3.6, is inloggen van buitenaf alleen mogelijk via Two Factor Authentication.

De conclusie is: *De Backend-omgeving voldoet deels aan norm 3.4, want de systeemaccounts zijn voorzien van gedegen wachtwoorden en worden gecontroleerd, maar zijn niet geïdentificeerd en gedocumenteerd*.

3.3.5. Wachtwoordbeleid

Norm 3.5 is: *De wachtwoordsyntax is sterk. Wachtwoorden verlopen periodiek*.

Wij hebben de volgende documentatie ontvangen:

3.5.a	Password Policy Production COVP	20-08-2020
3.5.b	Password Policy Acceptance COVA	20-08-2020
3.5.c	Password Policy Test COVT	20-08-2020

De door CIBG ingestelde wachtwoordsyntax bepaalt dat een wachtwoord aan ten minste vier richtlijnen dient te voldoen, zoals een vreemd teken, een hoofdletter, een cijfer en minimaal 14 karakters. Het wachtwoord is 42 dagen geldig.

In het tabblad ‘Account Policies/Password Policy’ in het document ‘Password syntax Default Domain Policy’ [doc 3.5.a t/m c] staat de actuele wachtwoordsyntax voor de drie omgevingen, namelijk Test, Acceptatie en Productie. Dit is op 20 augustus 2020:

Policy for Password	**Setting**
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 day
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

De conclusie is: *De Backend-omgeving voldoet aan norm 3.5, want er is een afgedwongen complexe wachtwoordsyntax en een expiratieperiode*.

3.3.6. Toegang van buitenaf

Norm 3.6 is: *Toegang van buitenaf is afgeschermd door middel van sterke identificatie en authenticatie*.

Ten tijde van ons onderzoek werd de bouwfase voor het Two Factor Authentication portal van KPN en CIBG afgerond. Het doel is dat CIBG via deze portal in kan loggen op de Backend-omgeving. Het portal is momenteel deels in gebruik.

De conclusie is: *Norm 3.6 is op dit moment niet van toepassing op de Backend-omgeving, aangezien deze nog wordt opgebouwd. Waarnemingen zijn pas in de toekomst mogelijk.*

3.3.7. Logging en Monitoring

Norm 3.7 is: *Logging en monitoring is aanwezig op de belangrijke functionaliteiten*.

Wij hebben de volgende documentatie ontvangen:

4.6.b	Alert Logic, 'Logmanagement incidents – Full Report'	01-04-2020
4.7.a	CIBG, 'CIBG logging beleid'	20-08-2020

KPN heeft een generiek beleid voor logging, dat is gespecificeerd in de KPN Security Policy (KSP). Deze policy is gepubliceerd op de website van KPN.

KPN verzorgt de monitoring van de netwerken en infrastructuur voor de Backend-omgeving.

CIBG heeft een beleid voor logging, dat is vastgelegd in het document 'CIBG logging beleid' [doc 4.7.a]. CIBG heeft twee verschillende logging systemen, namelijk:

- De normale Eventviewer logging op de servers;
- De logging op de ELK Stack. Deze log wordt beschikbaar gemaakt via een web portal op de beheerservers van de OTAP-omgeving.

Bij de ELK-logging moet worden geconfigureerd welke events in de Middleware of Eventviewer worden gelogd. Voor dit gedeelte is het bouwteam van het ministerie van VWS zelf verantwoordelijk.

Monitoring vanuit het CIBG gebeurt op server-niveau, namelijk via de task manager.

Wij hebben rapportages ontvangen, zoals 'Logmanagement incidents – Full Report' [doc 4.6.b], en de rapportages die zijn vermeld in de Sectie 3.4.7 en 3.4.8.

Ketenmonitoring wordt ingericht via het Security Operating Center (SOC). Aangezien die nog werd ingericht ten tijde van ons onderzoek, valt deze buiten de scope van ons onderzoek.

De conclusie is: *De Backend-omgeving voldoet aan norm 3.7, want logging en monitoring is aanwezig op de belangrijke functionaliteiten.*

3.4. IT General Controls

3.4.1. Certificaat services

Norm 4.1 is: *Alle vereiste certificaten zijn aanwezig en actueel*.

Wij hebben de volgende documentatie ontvangen:

4.1.a	CIBG, CIBG Certificaten Proces', versie 2.4	29-01-2020
4.1.b	Email, 'offerte HSMs voor COVID apps Offertenummer: 1064-08-2020-31-v2' (zonder financiële gegevens)	07-08-2020

De Certificate Services en Key Management processen zijn nog in ontwerpfase. Alle fysieke sleutels worden in de kluis bewaard, zowel bij KPN als bij CIBG.

De vijf Hardware Security Modules (HSM's) zijn geïnstalleerd. Wij hebben waargenomen dat de HSM's in de racks voor de Backend-omgeving zijn opgenomen in 'zone 1', en van KPN foto's ontvangen van de HSM's in 'zone 2'.

Tijdens ons onderzoek is de sleutelceremonie voor de HSM's voor de Test-omgeving doorlopen, namelijk op 28 augustus 2020. Wij zijn als auditors aanwezig geweest bij deze ceremonie, zowel bij Justid als bij CIBG.

Na afronding van ons onderzoek staan de sleutelceremonies gepland voor de Acceptatie- en Productie-omgeving. Wij zullen deze ceremonies ook bijwonen.

De conclusie is: *Norm 4.1 is nog niet van toepassing, aangezien de betreffende processen nog worden ontwikkeld en gebouwd. Wij hebben de aanwezigheid van de Hardware Security Modules (HSM's) waargenomen en als auditors de sleutelceremonie voor de HSM's voor de Test-omgeving bijgewoond.*

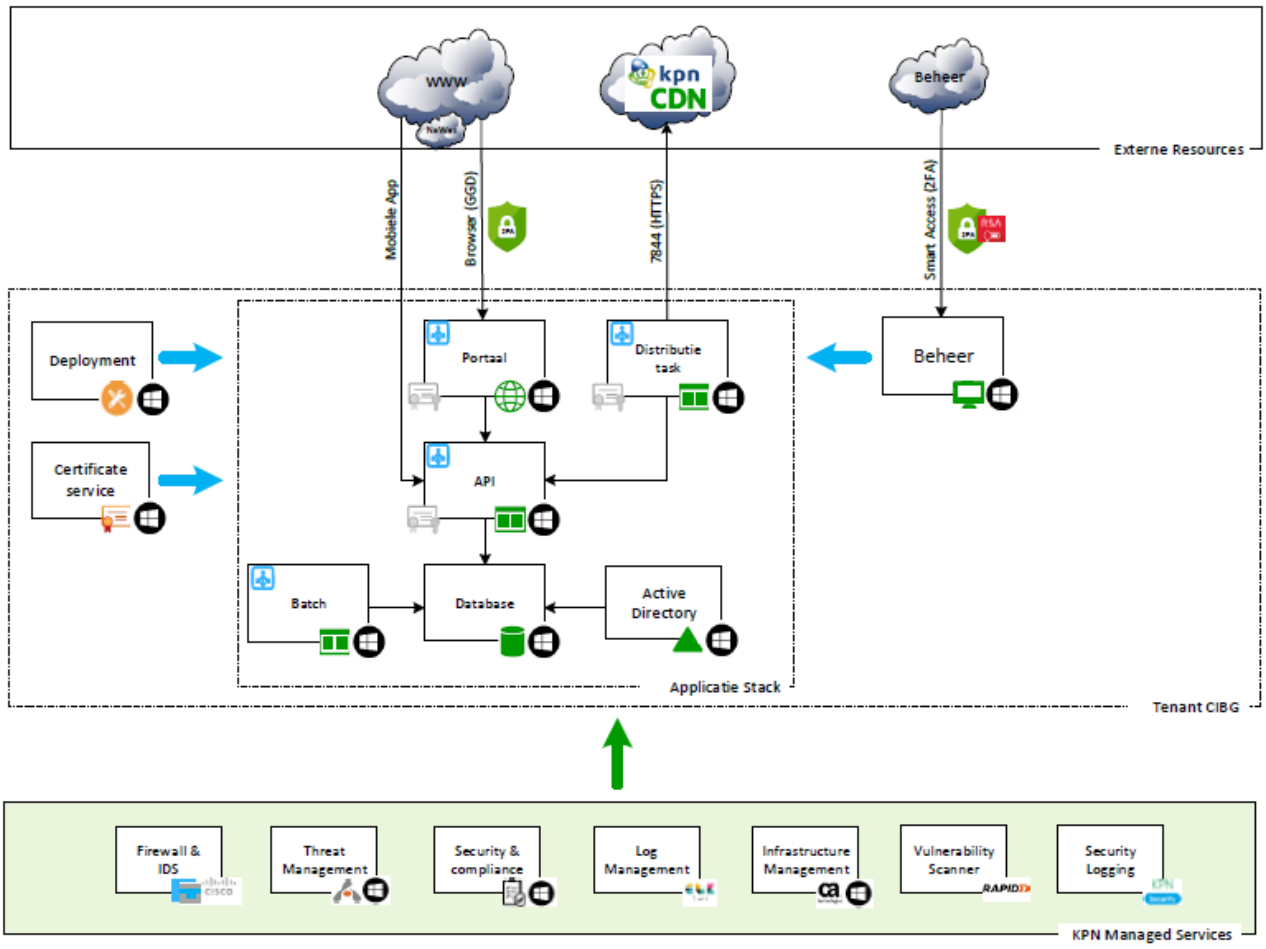
3.4.2. Sleutels ontvangen en vrijgeven

Norm 4.2 is: *Geïsoleerde omgevingen zijn ingericht om sleutels van mogelijk besmette personen te ontvangen, door GGD'en vrij te geven, en publiekelijk beschikbaar te stellen*.

Wij hebben de volgende documentatie ontvangen:

4.2.a	Github, 'Backend overview'	07-08-2020
4.2.b	Github, 'Merge remote-tracking branch private-master into feature private-to…'	07-08-2020

In de 'High Level Design Beschrijving' [doc 1.1.c] is de functionaliteit als volgt weergegeven in hoofdlijnen:



De Application Programming Interface (API) servers zitten achter de firewalls. KPN doet op de firewalls de Network Address Translation (NAT), zodat aan de binnenkant geen originele IP-adressen worden gebruikt.

De volgende processen zijn of worden ingericht:

- Throttling. Dit gebeurt op de firewalls met behulp van Threat Management, met de volgende instellingen:
  - Threat-detection rate: scanning-threat rate-interval 1200, average-rate 100, burst-rate 400;
  - Threat-detection rate: scanning-threat rate-interval 1800, average-rate 250, burst-rate 1000;
  - Conform de functionele eisen vanuit het ministerie van VWS gaat KPN op de firewalls de volgende thresholds implementeren:
    - Meer dan 100 requests/seconde voor langer dan 10 minuten, dan afknijpen;
    - Meer dan 250 requests van één IP address in een periode van 15 minuten, dan afknijpen.
- IP stripping. Dit gebeurt middels door de x-forwarded headers standaard niet door te sturen en verkeer via firewall-NAT, loadbalancer-NAT te laten verlopen. Zie ook Sectie 1.2 in het 'High Level Design Beschrijving' [doc 1.1.c].

De wettelijke eis voor het verwijderen van IP-informatie is 7 dagen. Doordat de IP-adressen aan de voorkant worden ge-NAT en gestript, voldoet de infrastructuur aan deze eis.

De conclusie is: *Norm 4.2 is nog niet van toepassing, aangezien de betreffende processen deels nog worden ontwikkeld en gebouwd.*

3.4.3. Fysieke beveiliging

Norm 4.3 is: *Alle IT-faciliteiten zijn beschermd in overeenstemming met hun belang*.

Wij hebben de volgende documentatie ontvangen:

4.3.a	Koninklijke KPN N.V., 'ISO 27001 – 2013 Hoofdcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	02-04-2020
4.3.b	KPN B.V., 'ISO 27001 – 2013 Kindcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	23-12-2019
4.3.c	Koninklijke KPN N.V. Elektronische Toegangsdiensten, 'ISO 27001 – 2013 Kindcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, dienst Elektronische Toegangsdiensten (vh eHerkenning), voor de rollen Middelenuitgever, Machtigingenregister, Authenticatiedienst en Herkenningsmakelaar voor de niveaus 1, 2, 2+, 3 en 4, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	23-12-2019
4.3.d	Noordbeek, 'Payment Card Industry (PCI) Data Security Standard, Attestation of Compliance for Onsite Assessments – Service Providers, Version 3.2.1, NorthC Datacenters'	01-03-2020
4.3.e	KPN, foto's 'Zone 2, racks met apparatuur van de Backend-omgeving'	28-08-2020
4.3.f	Ministerie VWS 'Quick Scan Informatiebeveiliging CoronaMelder TBB-2015 BIO-2018', versie 0.9	12-08-2020

3.4.3.1. Eisen voor fysieke beveiliging

Het ministerie van VWS heeft beperkte eisen geformuleerd voor het inrichten van de fysieke beveiliging van de datacenters. Dit heeft geleid tot het inrichten op Basisbeveiligingsniveau 2 (BBN2), conform de Baseline Informatiebeveiliging Overheid (BIO). BBN2 staat voor reguliere risico's en het beschermen van gegevens zoals die veelal binnen de overheid worden gebruikt.

Wij zijn het niet eens met de keuze voor BBN2. Naar onze mening ontbreken risicoanalyses die specifiek zijn gericht op Artikel 9 AVG 'bijzondere categorieën van persoonsgegevens', de weliswaar versleutelde maar toch soms herleidbare gezondheidsgegevens, het maatschappelijk vertrouwen in de CoronaMelder app en het internationale imago van de staat der Nederlanden.

Naar onze mening heeft het ministerie van VWS niet aangetoond waarom niet is gekozen voor Basisbeveiligingsniveau 3 (BBN3). Deze is in de BIO omschreven als (citaat):

- *BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie waarbij weerstand geboden*

moet worden tegen de dreiging, zoals Advanced Persistant Threat's (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien:

- *Het verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3.*

Onze risicoinschatting is dat statelijke actoren of andere dreigende actoren, zoals georganiseerde criminaliteit of activisten, interesse hebben in het stelen van de database of het verstoren van de processen. Naar onze mening kan het ministerie van VWS in het geval van een datalek door bijvoorbeeld diefstal van fysieke schijven of een succesvolle hack via een USB-stick de Nederlandse maatschappij en de internationale gemeenschap niet uitleggen waarom BBN3 niet is gehanteerd.

Ons standpunt met betrekking tot de noodzaak voor BBN3 wordt bevestigd door een interne Quick Scan op de CoronaMelder app [doc 4.3.f], waarin eveneens BBN3 wordt geadviseerd.

3.4.3.2. Aanvullende fysieke beveiligingsmaatregelen

Volgens de BIO wordt bij BBN3 rekening gehouden met het bieden van weerstand tegen statelijke actoren en geavanceerde aanvallen. Bij BBN3 worden de controls en overheidsmaatregelen uit BBN2 aangevuld met relevante eisen uit het 'Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie' (VIR-BI).

In het VIR-BI staat voor fysieke beveiliging onder andere (citaat):

- *Voor elke locatie, gebouw en ruimte waar zich bijzondere informatie bevindt, dient systematisch de beveiligingsmaatregelen in beeld te zijn gebracht voor fysieke toegangsbeheersing. Hierbij is ten minste voorzien in het aanbrengen van zonering c.q. compartimentering;*
- *Ten aanzien van zonering kunnen de diverse beveiligingszones worden onderkend, waarbij om toegang te krijgen tot ruimtes waarin bijzondere informatie wordt verwerkt, steeds zwaardere beveiligingsmaatregelen worden getroffen;*
- *Maatregel: Bijzondere informatie wordt zodanig behandeld en opgeslagen dat er een positief beveiligingsrendement is, op basis van schadeacceptatie en het dreigingsprofiel.*

Wij constateren dat er sprake is van een verhoogd risico voor de privacybescherming van de burgers met de CoronaMelder app en voor het imago van de staat, en dat rekening moet worden gehouden met statelijke actoren, beroepscriminelen, activisten etc. Daarvoor geldt het hogere niveau BBN3 en dienen aanvullende beveiligingsmaatregelen te worden getroffen conform het VIR-BI.

Wij adviseren het ministerie van VWS een risicoanalyse uit te voeren om vast te stellen of er sprake moet zijn van BBN2 of BBN3, en in het geval van BBN3 de daartoe vereiste aanvullende beveiligingsmaatregelen overeen te komen met KPN.

3.4.3.3. Site visit bij een datacenter

Wij hebben waarnemingen voor de fysieke beveiliging uitgevoerd op de locatie 'KPN Datacenter AM8 zone 1'. Voor de tweede locatie, 'zone 2', hebben wij het rapport 'Payment Card Industry (PCI) Data Security Standard, Attestation of Compliance for Onsite Assessments – Service Providers, Version 3.2.1, NorthC Datacenters' [doc 4.3.d] en door KPN gemaakte foto's van de racks met apparatuur van de Backend-omgeving [doc 4.3.e] ontvangen.

Conform de afspraken levert KPN geen dedicated fysieke servers, maar Managed Hosting. Het geleverde platform is managed Cloud NL VMWare op basis van de Windows 2016-standaard, met uitzondering van de ELK-servers welke Ubuntu draaien.

De voor de Backend-omgeving gebruikte datacenters van KPN beschikken over actuele certificaten voor compliance met ISO/IEC 27001:2013 'Information Security Management Systems Requirements' [doc 4.3.a t/m c].

Wij hebben tijdens onze assessment geen afwijkingen geconstateerd tussen de door KPN geleverde fysieke beveiligingsmaatregelen en de afspraken daarover met het ministerie van VWS, op het niveau BBN2.

Wij adviseren het ministerie van VWS niet te volstaan met onze huidige beperkte steekproef binnen deze assessment, maar een audit te laten uitvoeren op de fysieke beveiliging en de fysieke inrichting van de Backend-omgeving

De conclusie is: *De Backend-omgeving voldoet niet aan norm 4.3, aangezien niet alle IT-faciliteiten zijn beschermd overeenkomstig hun belang. Het ministerie van VWS heeft niet aangetoond waarom zij geen aanvullende maatregelen heeft geëist conform Basisbeveiligingsniveau 3 (BBN3). Naar onze mening zijn de huidige overeengekomen maatregelen conform BBN2 onvoldoende, gezien de verhoogde risico's.*

3.4.4. Configuratie Management

Norm 4.4 is: *De aanwezige hardware, software, parameters, versies etc. zijn vastgelegd*.

De operationele aspecten van de samenwerking tussen CIBG en KPN zijn beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a].

In Sectie 4.7 van dit document is Configuratie Management beschreven. Hierin staat als 'Specifieke afspraken' (citaat):

- *De opgebouwde kennis en de deployment geschiedenis van de gebruikte informatiesystemen en de configuratie van de systemen en netwerkcomponenten wordt door KPN vastgelegd en periodiek (per kwartaal) beschikbaar gesteld aan CIBG.*

De conclusie is: *De Backend-omgeving voldoet aan norm 4.4, want de aanwezige hardware, software, parameters, versies etc. zijn vastgelegd*.

3.4.5. Change Management

Norm 4.5 is: *Wijzigingen worden gestructureerd aangevraagd, voorbereid, geaccordeerd, getest en in productie genomen*.

Wij hebben de volgende documentatie ontvangen:

4.5.a	CIBG, 'CIBG Changemanagement procesbeschrijving', versie 2.0	19-07-2019

De operationele aspecten van de samenwerking tussen CIBG en KPN zijn beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. In Sectie 4.3 van dit document is Change Management beschreven.

CIBG beschikt over de 'CIBG Changemanagement procesbeschrijving' [doc 4.5.a].

Op 21 augustus 2020 is een Change Advisory Board (CAB) ingericht, die eenmaal of – indien nodig – tweemaal per dag overlegt over changes en incidenten. Tevens is een centraal meldpunt ingericht, dat 7x24 uur bereikbaar is.

Doordat de Backend-omgeving deels nog wordt ontworpen en gebouwd, verloopt Change Management voor de Backend-omgeving momenteel nog via de bouwteams. Het formele proces voor Change Management wordt in de toekomst in gebruik genomen.

De conclusie is: *De Backend-omgeving voldoet in opzet aan norm 4.5, want de processen voor Change Management zijn beschikbaar en er zijn afspraken gemaakt in de DAP. Wij hebben nog niet het bestaan kunnen toetsen, aangezien deze processen nog niet in gebruik zijn genomen.*

3.4.6. Incident en Problem Management (inclusief Security Incidenten)

Norm 4.6 is: *Incidenten worden afgehandeld, geregistreerd en geanalyseerd. Bij problemen wordt een root cause analysis uitgevoerd en vastgelegd*.

Wij hebben de volgende documentatie ontvangen:

4.6.a	CIBG, 'CIBG Incidentmanagement procesbeschrijving', versie 3.9	23-07-2019
4.6.b	Alert Logic, 'Logmanagement incidents – Full Report'	01-04-2020
4.6.c	RCA rapport CIBG-C2009 01014 – ticketref – INC9559030	15-09-2020
4.6.d	RCA – CT1222453 – CIBG-C2009 01100 – DDOS op DNS	16-09-2020

De operationele aspecten van de samenwerking tussen CIBG en KPN zijn beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. In Sectie 4.1 van dit document is Incident Management beschreven, en in Sectie 4.2 Problem Management.

CIBG beschikt over de 'CIBG Incidentmanagement procesbeschrijving' [doc 4.6.a].

De afhandeling van incidenten en problemen wordt gerapporteerd. Als steekproef hebben wij 'Logmanagement incidents – Full Report' [doc 4.6.b] ontvangen.

Met betrekking tot Security Incidenten hebben wij drie incidenten nagetrokken. Dat zijn een aanval met ransomware op de eigenaar van het datacenter, een Root Cause Analysis (RCA) voor traagheid door synchronisatieproblemen met de Midtier-cache [doc 4.6.c] en een RCA voor een DDoS-aanval [doc 4.6.d]. Wij hebben geconstateerd dat de afhandeling is verlopen conform de afspraken.

Doordat de Backend-omgeving deels nog wordt ontworpen en gebouwd, verlopen Incident en Problem Management voor de Backend-omgeving momenteel nog via de bouwteams. De formele processen voor Incident en Problem Management worden in de toekomst in gebruik genomen.

De conclusie is: *De Backend-omgeving voldoet in opzet aan norm 4.6, want de processen voor Incident en Problem Management zijn beschikbaar en er zijn afspraken gemaakt in de DAP. Wij hebben nog niet het bestaan kunnen toetsen, aangezien deze processen nog niet formeel in gebruik zijn genomen.*

3.4.7. Updates

Norm 4.7 is: *De meest recente updates en patches zijn geïnstalleerd.*

Wij hebben de volgende documentatie ontvangen:

4.7.a	CIBG, 'CIBG logging beleid'	20-08-2020
4.7.b	KPN, '2020 03 Shared Compas – Management-Overview'	01-04-2020
4.7.c	KPN, '2020 03 Algemeen Compas – Management-Overview'	01-04-2020
4.7.d	KPN, '2020 03 Beheer Compas – Management-Overview'	01-04-2020
4.7.e	KPN, '2020 03 Koppelvlak Compas – Management-Overview'	01-04-2020
4.7.f	KPN, '2020 03 SBV-Z Compas – Management-Overview'	01-04-2020
4.7.g	KPN, email, 'Windows Update Report – dela – 04_01_2020'	01-04-2020
4.7.h	KPN, email, 'Windows Update Report – VWS-ADR – 04_01_2020'	01-04-2020
4.7.i	KPN, email, 'Windows Update Report – VWS-Algemeen – 04_01_2020'	01-04-2020
4.7.j	KPN, email, 'Windows Update Report – VWS-Beheer – 04_01_2020'	01-04-2020
4.7.k	KPN, email, 'Windows Update Report – VWS-Donor – 04_01_2020'	01-04-2020
4.7.l	KPN, email, 'Windows Update Report – VWS-IGJ – 04_01_2020'	01-04-2020
4.7.m	KPN, email, 'Windows Update Report – VWS-Koppelvlak – 04_01_2020'	01-04-2020
4.7.n	KPN, email, 'Windows Update Report – VWS-SBVZ – 04_01_2020'	01-04-2020
4.7.o	KPN, email, 'Windows Update Report – VWS-Shared – 04_01_2020'	01-04-2020
4.7.p	KPN, email, 'Windows Update Report – VWS-Zorro – 04_01_2020'	01-04-2020

De operationele aspecten van de samenwerking tussen CIBG en KPN zijn beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. In Sectie 4.5 van dit document is Patch Management beschreven.

Over de voortgang van Patch Management wordt periodiek gerapporteerd. Als steekproef hebben wij een aantal rapporten [doc 4.7.b t/m p] ontvangen.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.7, want de meest recente updates en patches zijn geïnstalleerd.*

3.4.8. Hardening en vulnerability scans

Norm 4.8 is: *De richtlijnen voor hardening zijn gevolgd voor de relevante platformen. Vulnerability scans worden periodiek uitgevoerd*.

Wij hebben de volgende documentatie ontvangen:

4.8.a	KPN, 'CoronaMelder Hardening Baseline Controls, Windows Server 2016'	28-07-2020
4.8.b	KPN, 'CoronaMelder Hardening Summary, Windows Server 2016'	28-07-2020
4.8.c	KPN, 'Covid19 Hardening Summary'	20-08-2020
4.8.d	KPN, 'Covid19 Hardening Baseline Details'	20-08-2020
4.8.e	Nessus Scan Report, '2020 03 – KPN-VWS-SCHEDULED_3l41pi'	23-04-2020
4.8.f	Nessus Scan Report, '2020 03 – KPN-DR-SCHEDULED_1xdrue'	23-04-2020
4.8.g	Nessus Scan Report, '2020 03 – KPN-SBVZ-SCHEDULED_0cyaif'	23-04-2020
4.8.h	Nessus Scan Report, '2020 03 – KPN-VIR-SCHEDULED_0fzzgo'	23-04-2020

In het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a] staat onder andere (citaat): *Vulnerability scans worden regelmatig uitgevoerd ter verificatie van de patchlevels en het opsporen van overige bekende kwetsbaarheden*.

Wij hebben een aantal rapporten over vulnerability scans [doc 4.8.a t/m h] ontvangen, als steekproef. De scans op 28 juli 2020 bevatten nog een aantal non-compliance issues.

KPN heeft nieuwe scanrapporten {doc 4.8.c en d] toegezonden, met de volgende toelichting (citaat uit email):

- *We hebben een meer recente scan, daterend van 20 augustus 2020 die een beter resultaat laat zien (Zie bijlages). Op een aantal onderwerpen is het scan-resultaat nog niet wat wij graag zien, ook al is de overall score groen. Dit betreft met name Windows Firewall With Advanced Security. Deze scoort 52%;*
- *Wij willen graag de volgende toelichting geven op deze score:*
  - *De rapportages vanuit Easy2audit betreffende COVID 19 Hardening zijn rapportages gebaseerd op een scan inside-in. Dit betekent dat deze rapportage niet inzicht geven in het daadwerkelijke beveiligingsniveau, zoals gerealiseerd met bijvoorbeeld perimeter beveiliging middels centrale firewalling;*
  - *Van belang daarbij is dat middels netwerksegmentatie op centrale firewalls standaard al het verkeer wordt geblocked. Alleen middels ACLs op de firewall is er traffic mogelijk op basis van IP-poort combinaties tussen servers;*
  - *Wat verder opvalt als tweede punt, is dat er een aantal systemen in dit rapport voortkomen welke nog in oplevering zijn en nog geconfigureerd dienen te worden. Deze leveren daarmee een slechter beeld op dan uiteindelijk de echte situatie is;*
  - *Verder 'waardeert' Easy2audit een aantal systemen negatief (56,6%) vanuit het domain profile (server frontend interface) ten aanzien van de 'Firewall state is set to On'. De reden is dat Easy2audit controleer op basis van de local security policy of het aanzetten van de firewall middels een GPO is geregeld. Dat is bij een aantal systemen niet het geval, waarbij echter wel is vastgesteld dat de firewall op deze systemen actief is. De negatieve bevinding is daarmee dus onterecht voor deze systemen op dit punt;*

- *Ten slotte zijn er allerlei 'minor' zaken die tot een lage beoordeling leiden. Een voorbeeld: voor wat betreft de firewall logs in het public profiel gaat Easy2audit uit van een andere naam van de logfile (publicfw.log) waarbij er een naam pfirewall.log staat ingesteld (paden zijn wel identiek). Een score van 0% vanwege een afwijkende naam van de logfile van dit profiel is natuurlijk niet veelzeggend over de veiligheid en compliancy van een server.*

♦ *Concluderend zijn de volgende punten:*
- *Inside in scan, geen rekening houdend met centrale blocking en firewalling vanuit perimeterbeveiliging;*
- *Systemen zijn nog in oplevering en niet volledig geconfigureerd;*
- *Firewalls staan lokaal aan, maar niet via een group policy;*
- *Minor zaken als naamconventies voor logfiles.*

♦ *voor KPN vooralsnog geen aanleiding om op dit moment aanpassingen te doen anders dan al staan gepland (verdere uitrol en inrichting). Dit mede ook gezien de behaalde score boven de 80% als veilig wordt gezien en op basis van bovenstaande punten (en andere) alleen maar beter uitvalt in de praktijk.*

Tijdens de interviews is bevestigd dat de processen voor 'hardening en vulnerability scans' grotendeels zijn geïmplementeerd en nog verder worden verbeterd.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.8, want de richtlijnen voor hardening zijn gevolgd voor de relevante platformen en vulnerability scans worden periodiek uitgevoerd.*

3.4.9. Virussen

Norm 4.9 is: *Antivirus is aanwezig op alle apparatuur waarvoor die is bedoeld.*

Wij hebben de volgende documentatie ontvangen:

4.9.a	CIBG, '20200401 – McAfee CIBG Rapportage'	01-04-2020

Antivirus-software van McAfee is geïnstalleerd. Er wordt periodiek gerapporteerd over antivirus, zoals blijkt uit het als steekproef ontvangen rapport [doc 4.9.a].

De conclusie is: *De Backend-omgeving voldoet aan norm 4.9, Antivirus is aanwezig op alle apparatuur waarvoor die is bedoeld.*

3.4.10. Firewall

Norm 4.10 is: *Een firewall of DMZ is aanwezig en de rule set wordt onderhouden*.

Wij hebben de volgende documentatie ontvangen:
4.10.a Cisco, 'Firepower Report mijn.donorregister.nl-20200401083002-1609' 01-04-2020

KPN levert dedicated managed firewalls voor de Backend-omgeving.

Het proces voor 'wijzigingen op de firewall rules' is beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. Hierin staat tevens (citaat):

- *De dedicated Firewall voor VWS, een cluster van Cisco ASA 5516-x nodes, is voorzien van Firepower Analytics & Automation. Het Firepower managementcentrum verzamelt, correleert en toont contextuele informatie over alles wat in de VWS omgeving draait en in het netwerk veranderd. Het correleert automatisch beveiligingsgebeurtenissen met de kwetsbaarheden in het netwerk.*

Het Intrusion Detection System (IDS) is ingericht en operationeel. In de DAP [doc 2.1.a] staat als toelichting (citaat):

- *IDS wordt doorlopend bijgewerkt met informatie over nieuwe kwetsbaarheden, beschermt systemen en applicaties tegen het benutten van deze kwetsbaarheden door kwaadwillende en rapporteert daarover. Op basis van verschillende beschermingselementen worden netwerkverkeersstromen geanalyseerd en wanneer relevant gerapporteerd. Hierbij brengt IDS de verschillende systemen en applicaties binnen het netwerk doorlopend in kaart. Zo kunnen er op eenvoudige wijze systeem- en applicatie-specifieke beschermingselementen en parameters worden ingesteld en geactiveerd voor reeds bestaande en mogelijk toekomstige kwetsbaarheden met betrekking tot deze systemen en applicaties. De beschermingselementen kunnen daarna op basis van bedrijfsrisico en relevantie van deze systemen en applicaties worden geprioriteerd;*
- *Door de installatie van certificaten worden ook versleutelde netwerkverkeersstromen geïnspecteerd door IDS;*
- *Op basis van de ingestelde beschermingselementen en parameters worden door IDS intrusion incidenten aangemaakt. Deze incidenten krijgen een impact level;*
- *Een keer per maand wordt een IDS rapportage (Firepower Report) gegenereerd welke onderdeel uitmaakt van de maandelijkse Security Rapportage en welke maandelijks tijdens het Security Overleg wordt besproken.*

Het Intrusion Prevention System (IPS) is nog niet operationeel. Ten tijde van ons onderzoek draaide IPS nog met IDS in 'learning mode'.

Als steekproef hebben wij de rapportage 'Firepower Report mijn.donorregister.nl-20200401083002-1609' [doc 4.10.a] ontvangen.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.10, want een firewall of DMZ is aanwezig en de rule set wordt onderhouden*.

3.4.11. Penetratietest

Norm 4.11 is: *Recentelijk is een penetratietest uitgevoerd*.

Wij hebben de volgende documentatie ontvangen:

4.11.a	IT Forensics & Incident Response (NFIR B.V.), 'Rapportage Penetratietest', Projectnaam 20060 – Melun, versie 1.0	29-07-2020
4.11.b	Ministerie van Infrastructuur en Waterstaat, Bestuurskern, DCI, Standaard Platform / Cloud Services, memo 'Corona Notificatie-app Website – PEN-test'	10-07-2020
4.11.c	HackDefense, 'Testrapport penetratietest CoronaMelder', versie 1.0	15-07-2020
4.11.d	Cholet, 'Bevindingen penetratietest 20063 – Grey Box'	17-08-2020

Penetratietesten en codereviews zijn en worden uitgevoerd.

Wij hebben vier rapportages ontvangen vanuit de pentesten, die hierboven zijn gespecificeerd. Via een steekproef op de interne communicatie tussen CIBG, KPN en de pentesters hebben wij vastgesteld dat verbeteracties worden uitgevoerd voor via de pentesten gesignaleerde zwakheden. Ten tijde van ons onderzoek liep nog een hertest voor een van de pentesten.

De bouwteams bij CIBG en KPN hanteren een log voor Risks, Actions, Issues and Decisions (RAID) voor geconstateerde issues. Wij hebben op het scherm kennis genomen van de inhoud van deze log, die doorlopend wordt geactualiseerd tijdens het inrichtingsproces.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.11, want recentelijk zijn penetratietesten uitgevoerd*.

3.4.12. Monitoring van de beschikbaarheid van systemen

Norm 4.12 is: *De systemen worden gemonitord op beschikbaarheid*.

Het proces voor monitoring van de beschikbaarheid is beschreven in Sectie 4.11 van het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. Hierin staat onder andere (citaat):

- *De infrastructuur wordt 24x7 gemonitord op zowel componentniveau als op dienst/keten niveau waarbij real time performance en beschikbaarheid zichtbaar zijn. Deze bewaking kan voor bepaalde applicaties en websites 7x24 uur zijn. Tijdens de bewaking wordt iemand gewaarschuwd bij een verstoring en er is altijd een aangewezen aanspreekpunt bereikbaar voor afnemers of medewerkers van CIBG die support kan geven. Minimaal zal (ook) op systeemsoftware of operating systeemniveau bewaakt moeten worden;*
- *Vanuit haar verantwoordelijkheid voor de operationele dienstverlening draagt de hosting partij zorg voor de correcte inrichting van monitoring op systeem- en monitoring op applicatieniveau conform de instructies van CIBG. CIBG heeft realtime inzage in de monitoring tool;*
- *Informatie over verstoringen buiten kantoortijden wordt per e-mail doorgestuurd naar medewerkers van CIBG. Bij prioriteit 1 meldingen geconstateerd door KPN wordt tevens telefonisch contact opgenomen met de medewerker van het CIBG zoals vermeld in de wie-is-wie*

lijst. Medewerkers van CIBG kunnen via een web-interface kijken naar de beschikbaarheid en prestaties van bewaakte systemen, vanaf elke willekeurige locatie over het internet.

Monitoring vanuit het CIBG gebeurt op server-niveau, namelijk via de task manager.

Tijdens de interviews is bevestigd dat het proces voor de monitoring van beschikbaarheid aanwezig is. Dit wordt verder op maat gesneden voor de Backend-omgeving van de CoronaMelder.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.12, want de systemen worden gemonitord op beschikbaarheid.*

3.4.13. OTAP

Norm 4.13 is: *Het principe van Ontwikkel, Test, Acceptatie en Productie (OTAP) wordt toegepast*.

KPN heeft een OTAP-straat ingericht voor het ministerie van VWS, waarop het ministerie zelf Application Development en Application Management uitvoert.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.13, want het principe van OTAP wordt toegepast.*

3.4.14. Testgegevens

Norm 4.14 is: *Testgegevens bevatten geen identificerende persoonsgegevens*.

De applicatiesoftware en data vallen onder de verantwoordelijkheid van het ministerie van VWS. De testgegevens vallen daarom buiten de scope van ons onderzoek naar de Backend-omgeving.

De conclusie is: *Norm 4.14 in niet van toepassing, aangezien de testgegevens buiten de scope van dit onderzoek vallen.*

3.4.15. Service Level Agreement (SLA)

Norm 4.15 is: *SLA's of onderhoudscontracten zijn aanwezig voor de kritieke onderdelen binnen de IT*.

De dienstverlening van KPN aan CIBG is beschreven in het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a]. Het contract is de 'Raamovereenkomst ARBIT-2016 tussen Ministerie van Volksgezondheid, Welzijn en Sport, CIBG, IGZ en ESIT, en KPN B.V. inzake Managed Hosting & Storage services met kenmerk 201700274.068' [doc 1.1.e].

De conclusie is: *De Backend-omgeving voldoet aan norm 4.15, want een contract en een DAP zijn aanwezig voor de kritieke onderdelen binnen de IT.*

3.4.16. Service Level Reporting (SLR)

Norm 4.16 is: *Over de IT-diensten van derden wordt gerapporteerd. De rapportage wordt geevalueerd op het voldoen aan de gemaakte prestatie-afspraken*.

In het 'Dossier Afspraken en Procedures (DAP)' [doc 2.1.a] zijn de periodieke rapportages besproken, evenals de overlegstructuur. Hierin staat onder andere in Sectie 2.2 (citaat):

- *Er zullen maandelijks Service Level (zie bijlage 2) en Security- rapportages worden geleverd uiterlijk op de 10de werkdag van de volgende maand door KPN (waarin onder andere beschikbaarheid en andere SLA parameters). Deze worden iedere maand besproken in een tactisch en security overleg. Verbeterpunten worden door KPN aangedragen en opgepakt op basis van een Service Improvement plan;*
- *Op verzoek van CIBG kan te allen tijde overleg plaatsvinden waarbij medewerkers van CIBG direct contact hebben met de medewerkers van KPN en gezamenlijk verbeterpunten opstellen.*

Tijdens de interviews is bevestigd dat het proces voor rapportage over de dienstverlening aanwezig is, evenals een overlegstructuur.

De conclusie is: *De Backend-omgeving voldoet aan norm 4.16, want over de IT-diensten van derden wordt gerapporteerd en de rapportage wordt geëvalueerd op het voldoen aan de gemaakte prestatie-afspraken.*

3.5. Continuïteit, backup en recovery

3.5.1. Continuïteitsplannen

Norm 5.1 is: *Procedures en plannen zijn vastgesteld en gedocumenteerd*.

In de 'High Level Design Beschrijving' [doc 1.1.c] is de Sectie 'Continuïteit en beschikbaarheid' opgenomen. Hierin is vermeld (citaat):

- *Er wordt een beschikbaarheid van 99,9% uitgevraagd. Ten behoeve van deze eis en de opbouw van andere dienstverlening voor CIBG is gekozen voor de standaardoplossing om de omgeving redundant over 2 datacenters te verdelen. Dit zorgt voor een hoge beschikbaarheid en een geografische redundantie van de dubbel uitgevoerde componenten binnen het landschap. Daarbij biedt dit ook een hoge beschikbaarheid in de totaalketen van componenten van welke de App gebruik maakt. Dit betekent automatisch ook dat er geen sprake is van een uitwijk. Bij uitval van 1 datacenter zullen de redundante onderdelen op het 2de datacenter voorzien in een volledige functionele stack om de CoronaMelder beschikbaar te houden.*
- *Back-up is in overeenstemming met afspraak gelimiteerd op een retentie van 14 dagen, waarbij er van alle virtuele servers binnen het hosting onderdeel dagelijks snapspots worden gemaakt welke offsite zijn opgeslagen.*

De eis van 14 dagen in de laatste zin is aangepast naar een retentieperiode van maximaal 7 dagen.

Tijdens de interviews is bevestigd dat de failover is ingericht.

De conclusie is: *De Backend-omgeving voldoet aan norm 5.1, want procedures en plannen zijn vastgesteld voor de failover en gedocumenteerd.*

3.5.2. Back-up

Norm 5.2 is: *Het back-up-proces is ingericht en back-ups worden periodiek uitgevoerd*.

Van alle virtuele servers binnen het hosting onderdeel worden dagelijks snapspots gemaakt, welke offsite zijn opgeslagen.

De conclusie is: *De Backend-omgeving voldoet aan norm 5.2, want het back-up-proces is ingericht.*

3.5.3. Recovery

Norm 5.3 is: *Periodiek worden restore-testen uitgevoerd voor de back-ups*.

De twee productie-omgevingen kennen ieder een gespiegelde colocatie. Deze gekruiste configuratie faciliteert een failover, indien een productie-omgeving down gaat.

De conclusie is: *Norm 5.3 is niet van toepassing, gezien de aanwezigheid van colocaties en een failover.*

3.5.4. Uitwijk naar andere locatie

Norm 5.4 is: *Een uitwijklocatie is aanwezig en het uitwijkproces is getest*.

Wij hebben de volgende documentatie ontvangen:

5.4.a	CIBG, 'CoronaMelder – Verslag Failover Test ACC'	18-09-2020

De twee productie-omgevingen kennen ieder een gespiegelde colocatie. Deze gekruiste configuratie faciliteert een failover, indien een productie-omgeving (PROD) down gaat.

Op 18 september 2020 is een failover-test uitgevoerd op de COVA-omgeving van de CoronaMelder, namelijk de acceptatie-omgeving (ACC) [doc 5.4.a]. Hierbij bleken enkele manco's, die vervolgens zijn opgelost.

Ten tijde van ons onderzoek was de planning voor de activiteiten in relatie tot de failover-testen:
- 1 oktober 2020: Oplevering aanpassingen van ACC + PROD;
- 5 oktober 2020: Hertest van ACC;
- 7 oktober 2020: Test van PROD.

De conclusie is: *De Backend-omgeving voldoet aan norm 5.4, want het uitwijkproces is aanwezig en getest.*

3.5.5. Robuustheid DDoS

Norm 5.5 is: *Maatregelen zijn ingericht om een DDoS-aanval te kunnen weerstaan*.

Wij hebben de volgende documentatie ontvangen:

5.5.a	NBIP, 'Bescherming tegen DDoS-aanvallen, NaWas: de Nationale anti-DDoS Wasstraat', versie V5-001	15-01-2020

KPN participeert in de Nationale anti-DDoS Wasstraat (NaWas). Een beschrijving van de maatregelen staat in Bescherming tegen DDoS-aanvallen, NaWas: de Nationale anti-DDoS Wasstraat' [doc 5.5.a].

De conclusie is: *De Backend-omgeving voldoet aan norm 5.5, want maatregelen zijn ingericht om een DDoS-aanval te kunnen weerstaan.*

Bijlage A Overzicht van interviews en waarnemingen

In het kader van de privacy van de geïnterviewde en betrokken functionarissen zijn hieronder alleen hun functies benoemd.

Nr.	Functie	Datum
1.	Opdrachtgever, ministerie van VWS	Dagelijks
2.	Projectleider, ministerie van VWS	23-09-2020 + Emails
3.	Applicatiemanager, Afdeling Applicatie- en servicemanagement, CIBG	17-08-2020 20-08-2020
4.	Contract- en Leveranciersmanager, CIBG	20-08-2020
5.	Teamleider, CIBG	26-08-2020 27-08-2020
6.	Technische Beheerders, Afdeling ICT, CIBG	28-08-2020 + Emails
7.	Projectleider HSM, DICTU	28-08-2020 + Emails
8.	Senior Information Architect, Justid, Ministerie van Justitie en Veiligheid	28-08-2020 + Emails
9.	Vakmanager, CO CM IT KIS, KPN	Tweedagelijks
10.	Vakmanager, ACN DCI Infra Tech KIS, KPN	24-08-2020
11.	Manager Operations, S&D Cloud Services, KPN	24-08-2020
12.	Technisch beheerder, S&D Cloud Services, KPN	Emails
13.	Projectmanager, CO CM IT KIS, KPN	17-08-2020

Nr.	Waarneming	Datum
1.	KPN Datacenter AM8 zone 1 (gebouw van Equinix)	21-08-2020
2.	HSM sleutelceremonie: Justitiële Informatiedienst (Justid), Ministerie van Justitie en Veiligheid	28-08-2020
3.	HSM sleutelceremonie: Agentschap CIBG, Uitvoeringsorganisatie van VWS, Afdeling Applicatie- en servicemanagement	28-08-2020 01-09-2020

Bijlage B Lijst van geraadpleegde documentatie en steekproeven

Wij hebben de volgende documentatie ontvangen, waarbij de stukken zijn genummerd conform ons werkprogramma voor de assessment:

Nr.	Dossierstuk	Datum
1.1.a	KPN, 'CoronaMelder App VWS – CIBG – High Level Design (HLD)', versie 0.29	23-07-2020
1.1.b	KPN, 'VWS – CIBG – CoronaMelder App Low Level Design (LLD)', versie 0.15	29-07-2020
1.1.c	KPN, 'High Level Design Beschrijving, Ministerie van VWS – CIBG, CoronaMelder App', versie 0.2	18-08-2020
1.1.d	CIBG, 'Corona App – Functioneel-Technisch Ontwerp', versie 0.7	14-08-2020
1.1.e	'Raamovereenkomst ARBIT-2016 tussen Ministerie van Volksgezondheid, Welzijn en Sport, CIBG, IGZ en ESIT, en KPN B.V. inzake Managed Hosting & Storage services met kenmerk 201700274.068'	23-05-2017
1.3.a	'Programma van Eisen voor een digitale oplossing ter aanvulling op bron- en contactonderzoek', versie 0.5	19-05-2020
1.3.b	Kamerbrief bijlage, Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19, 'Advies 1: Programma van Eisen voor digitale oplossing ter aanvulling op bron- en contactonderzoek GGD', versie 0.4	16-07-2020
2.1.a	KPN, 'Dossier Afspraken en Procedures (DAP) CIBG (een agentschap van Ministerie VWS)', versie 1.7	04-02-2020
2.2.a	Ministerie van VWS, Kamerbrief, 'Landelijke introductie CoronaMelder', kenmerk 1722926-208233-DICIO	16-07-2020
2.2.b	Ministerie van VWS, 'Statusslide minister', versie 15.25	06-07-2020
2.2.c	Ministerie van VWS, 'Statusslide minister', versie 15.00	09-07-2020
2.2.d	Ministerie van VWS, 'Statusslide minister', versie 18.30-2	13-07-2020
2.2.e	Ministerie van VWS, 'Dashboard minister', versie 17.30	20-07-2020
2.2.f	Ministerie van VWS, 'Dashboard minister', versie 22.00-2	03-08-2020
2.2.g	Stuurgroep agenda's VWS, CIBG en KPN, juli, augustus en september 2020	17-07-2020 04-09-2020
2.2.h	CIBG, Offerte Hosting Coronamelder, definitief	06-08-2020
2.2.i	Bijlage I. Reactie offerte 20 augustus 2020	20-08-2020
2.2.j	Bijlage II. Monitoring proposal backend CoronaMelder	02-09-2020
2.2.k	Bijlage III. Referentiegids covid-19 HSM beheer, versie 0.5	27-08-2020
2.2.l	Bijlage IV. Inrichting infrastructuur Datacenters covid-19 HSM beheer, versie 1.1	26-08-2020
2.2.m	Ministerie van VWS, Brief Reactie CIBG inzake offerte 20 augustus 2020	07-09-2020
2.2.n	Verslag sessie COVID-19 app rol CIBG	15-07-2020
2.3.a	Spreadsheet, 'FMEA CoronaMelder risicoinschatting' (geen vermelding van auteur of versie)	-
2.3.b	Github, 'Baseline for the Proof of Concept'	06-07-2020
2.3.c	Github, 'FMEA CoronaMelder'	23-09-2020
2.4.a	Ministerie van VWS, 'Compliancyrapport implementatie verplichte webeisen CoronaMelder', versie 1.1	16-07-2020

Nr.	Dossierstuk	Datum
2.4.b	CIBG, 'Strategisch beleidsdocument informatieveiligheid', versie 1.0	12-11-2018
2.4.c	CIBG, 'CIBG SSD Requirements, Security Requirements binnen Secure Software Development', versie 2.8	08-11-2019
2.4.d	CIBG, 'Overzicht en Planning Security Rapportage voor CIBG over het jaar 2019'	14-11-2019
2.4.e	KPN Security, 'Maandelijkse security rapportage van de systemen van het CIBG over het eerste kwartaal 2020'	16-04-2020
2.5.a	Ministerie van VWS, Directie Informatiebeleid, CIO 'Gegevensbeschermingseffectbeoordeling (DPIA) COVID-19 notificatie-app', vastgesteld	07-07-2020
2.5.b	Ministerie van VWS, 'Privacy Governance 2018', versie 1.2	28-11-2018
2.5.c	Ministerie van VWS, 'Draaiboek Incidenten en Datalekken VWS', versie 1.1	23-01-2020
2.5.d	Ministerie van VWS, Panel van burgers, 'Ethische analyse van de COVID-19 notificatie app ter aanvulling op bron en contactonderzoek GGD'	14-07-2020
3.1.a	CIBG, 'Uitdraai 2020 03 CIBG Active Directory'	01-04-2020
3.1.b	Noordbeek, 'Analyserapport Active Directory COVP'	20-08-2020
3.2.a	CIBG, 'Autorisatiebeheer generieke tooling en infrastructuur', versie 0.1	05-08-2020
3.5.a	Password Policy Production COVP	20-08-2020
3.5.b	Password Policy Acceptance COVA	20-08-2020
3.5.c	Password Policy Test COVT	20-08-2020
4.1.a	CIBG, CIBG Certificaten Proces', versie 2.4	29-01-2020
4.1.b	Email, 'offerte HSMs voor COVID apps Offertenummer: 1064-08-2020-31-v2' (zonder financiële gegevens)	07-08-2020
4.2.a	Github, 'Backend overview'	07-08-2020
4.2.b	Github, 'Merge remote-tracking branch private-master into feature private-to…'	07-08-2020
4.3.a	Koninklijke KPN N.V., 'ISO 27001 – 2013 Hoofdcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	02-04-2020
4.3.b	KPN B.V., 'ISO 27001 – 2013 Kindcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	23-12-2019
4.3.c	Koninklijke KPN N.V. Elektronische Toegangsdiensten, 'ISO 27001 – 2013 Kindcertificaat', afgegeven door DNV GL, met als scope 'Het initieel en continu leveren van telecommunicatie- en informatiediensten aan de zakelijke markt, dienst Elektronische Toegangsdiensten (vh eHerkenning), voor de rollen Middelenuitgever, Machtigingenregister, Authenticatiedienst en Herkenningsmakelaar voor de niveaus 1, 2, 2+, 3 en 4, in overeenstemming met de Verklaring van Toepasselijkheid v3.18, d.d. 31-10-2019'	23-12-2019
4.3.d	Noordbeek, 'Payment Card Industry (PCI) Data Security Standard, Attestation of Compliance for Onsite Assessments – Service Providers, Version 3.2.1, NorthC Datacenters'	01-03-2020

Nr.	Dossierstuk	Datum
4.3.e	KPN, foto's 'Zone 2, racks met apparatuur van de Backend-omgeving'	28-08-2020
4.3.f	Ministerie VWS 'Quick Scan Informatiebeveiliging CoronaMelder TBB-2015 BIO-2018', versie 0.9	12-08-2020
4.5.a	CIBG, 'CIBG Changemanagement procesbeschrijving', versie 2.0	19-07-2019
4.6.a	CIBG, 'CIBG Incidentmanagement procesbeschrijving', versie 3.9	23-07-2019
4.6.b	Alert Logic, 'Logmanagement incidents – Full Report'	01-04-2020
4.7.a	CIBG, 'CIBG logging beleid'	20-08-2020
4.7.b	KPN, '2020 03 Shared Compas – Management-Overview'	01-04-2020
4.7.c	KPN, '2020 03 Algemeen Compas – Management-Overview'	01-04-2020
4.7.d	KPN, '2020 03 Beheer Compas – Management-Overview'	01-04-2020
4.7.e	KPN, '2020 03 Koppelvlak Compas – Management-Overview'	01-04-2020
4.7.f	KPN, '2020 03 SBV-Z Compas – Management-Overview'	01-04-2020
4.7.g	KPN, email, 'Windows Update Report – dela – 04_01_2020'	01-04-2020
4.7.h	KPN, email, 'Windows Update Report – VWS-ADR – 04_01_2020'	01-04-2020
4.7.i	KPN, email, 'Windows Update Report – VWS-Algemeen – 04_01_2020'	01-04-2020
4.7.j	KPN, email, 'Windows Update Report – VWS-Beheer – 04_01_2020'	01-04-2020
4.7.k	KPN, email, 'Windows Update Report – VWS-Donor – 04_01_2020'	01-04-2020
4.7.l	KPN, email, 'Windows Update Report – VWS-IGJ – 04_01_2020'	01-04-2020
4.7.m	KPN, email, 'Windows Update Report – VWS-Koppelvlak – 04_01_2020'	01-04-2020
4.7.n	KPN, email, 'Windows Update Report – VWS-SBVZ – 04_01_2020'	01-04-2020
4.7.o	KPN, email, 'Windows Update Report – VWS-Shared – 04_01_2020'	01-04-2020
4.7.p	KPN, email, 'Windows Update Report – VWS-Zorro – 04_01_2020'	01-04-2020
4.8.a	KPN, 'CoronaMelder Hardening Baseline Controls, Windows Server 2016'	28-07-2020
4.8.b	KPN, 'CoronaMelder Hardening Summary, Windows Server 2016'	28-07-2020
4.8.c	KPN, 'Covid19 Hardening Summary'	20-08-2020
4.8.d	KPN, 'Covid19 Hardening Baseline Details'	20-08-2020
4.8.e	Nessus Scan Report, '2020 03 – KPN-VWS-SCHEDULED_3l41pi'	23-04-2020
4.8.f	Nessus Scan Report, '2020 03 – KPN-DR-SCHEDULED_1xdrue'	23-04-2020
4.8.g	Nessus Scan Report, '2020 03 – KPN-SBVZ-SCHEDULED_0cyaif'	23-04-2020
4.8.h	Nessus Scan Report, '2020 03 – KPN-VIR-SCHEDULED_0fzzgo'	23-04-2020
4.9.a	CIBG, '20200401 – McAfee CIBG Rapportage'	01-04-2020
4.10.a	Cisco, 'Firepower Report mijn.donorregister.nl-20200401083002-1609'	01-04-2020
4.11.a	IT Forensics & Incident Response (NFIR B.V.), 'Rapportage Pene-tratietest', Projectnaam 20060 – Melun, versie 1.0	29-07-2020
4.11.b	Ministerie van Infrastructuur en Waterstaat, Bestuurskern, DCI, Standaard Platform / Cloud Services, memo 'Corona Notificatie-app Website – PEN-test'	10-07-2020
4.11.c	HackDefense, 'Testrapport penetratietest CoronaMelder', versie 1.0	15-07-2020
4.11.d	Cholet, 'Bevindingen penetratietest 20063 – Grey Box'	17-08-2020
5.4.a	CIBG, 'CoronaMelder – Verslag Failover Test ACC'	18-09-2020

Nr.	Dossierstuk	Datum
5.5.a	NBIP, ‘Bescherming tegen DDoS-aanvallen, NaWas: de Nationale anti-DDoS Wasstraat’, versie V5-001	15-01-2020

Bijlage C Het werkprogramma

Het onderstaande door ons ontwikkelde werkprogramma voor het inventariseren van de beheersingsmaatregelen in relatie tot de eisen voor informatiebeveiliging en privacybescherming is gericht op het verkrijgen van de mate van inzicht dat nodig is voor het leveren van publieke transparantie.

ID	Onderwerp	Norm voor controlemaatregel
1	**De IT omgeving**	
1.1	Beschrijving IT-omgeving	De huidige IT-omgeving is in voldoende mate beschreven.
1.2	Toekomst	Ontwikkelingen in de IT-omgeving in de nabije toekomst zijn bekend.
1.3	Eisen en wensen	De eisen en wensen voor de IT-omgeving zijn bekend.
2	**Besturing, Interne IT-beheersing en IT Governance**	
2.1	Strategie en beleid	De IT-strategie is afgestemd op de actuele situatie van de organisatie. In het IT-beleid zijn concrete doelen en resultaten benoemd.
2.2	IT-organisatie en Control	De organisatie bewaakt de uitvoering van de IT-strategie, het IT-beleid en de IT-procedures, en de voortgang van projecten.
2.3	Risicobeheersing	De organisatie heeft de IT-risico's geanalyseerd en de mitigerende maatregelen vastgelegd.
2.4	Informatiebeveiliging	De organisatie voldoet aantoonbaar aan ISO/IEC 27001:2013, de NIB-richtlijn en de Cyber Security Act.
2.5	Privacybescherming	Persoonsgegevens worden adequaat behandeld en beschermd, conform doelbinding, proportionaliteit en subsidiariteit. De in de DPIA voorgestelde maatregelen zijn gerealiseerd.
2.6	Opvolging van voorgaande audit aanbevelingen	De aanbevelingen uit audits zijn opgevolgd of er zijn verbeterplannen.
3	**Accountbeheer en wachtwoordbeleid**	
3.1	Accountbeheer	Accounts worden individueel toegekend. Er worden geen groepsaccounts gebruikt. Een overzicht van alle accounts is beschikbaar.
3.2	Instroom, doorstroom en uitstroom	Accounts worden tijdig aangemaakt, gemuteerd, geblokkeerd en verwijderd, conform de personele wijzigingen.
3.3	Key-gebruikers- en administratoraccounts	Key-users en administrators gebruiken sterke wachtwoorden of Two Factor Authentication.
3.4	Systeemaccounts	Voor systeemaccounts is geborgd dat geen misbruik mogelijk is.
3.5	Wachtwoordbeleid	De wachtwoordsyntax is sterk. Wachtwoorden verlopen periodiek.
3.6	Toegang van buitenaf	Toegang van buitenaf is afgeschermd door middel van sterke identificatie en authenticatie.
3.7	Logging	Logging is aanwezig op de belangrijke functionaliteiten.

ID	Onderwerp	Norm voor controlemaatregel
4	**IT General Controls**	
4.1	Certificaat services	Alle vereiste certificaten zijn aanwezig en actueel.
4.2	Sleutels ontvangen en vrijgeven	Geïsoleerde omgevingen zijn ingericht om sleutels van mogelijk besmette personen te ontvangen, door GGD'en vrij te geven, en publiekelijk beschikbaar te stellen.
4.3	Fysieke beveiliging	Alle IT-faciliteiten zijn beschermd in overeenstemming met hun belang.
4.4	Configuratie Management	De aanwezige hardware, software, parameters, versies etc. zijn vastgelegd.
4.5	Change Management	Wijzigingen worden gestructureerd aangevraagd, voorbereid, geaccordeerd, getest en in productie genomen.
4.6	Incident en Problem Management	Incidenten worden afgehandeld, geregistreerd en geanalyseerd. Bij problemen wordt een root cause analysis uitgevoerd en vastgelegd.
4.7	Updates	De meest recente updates en patches zijn geïnstalleerd.
4.8	Hardening en vulnerability scans	De richtlijnen voor hardening zijn gevolgd voor de relevante platformen. Vulnerability scans worden periodiek uitgevoerd.
4.9	Virussen	Antivirus is aanwezig op alle apparatuur waarvoor die is bedoeld.
4.10	Firewall	Een firewall of DMZ is aanwezig en de rule set wordt onderhouden.
4.11	Penetratietest	Een penetratietest is recentelijk uitgevoerd.
4.12	Monitoring van de beschikbaarheid	De systemen worden gemonitord op beschikbaarheid.
4.13	OTAP	Het principe van Ontwikkel, Test, Acceptatie en Productie (OTAP) wordt toegepast.
4.14	Testgegevens	Testgegevens bevatten geen identificerende persoonsgegevens.
4.15	Service Level Agreement (SLA)	SLA's of onderhoudscontracten zijn aanwezig voor de kritieke onderdelen binnen de IT.
4.16	Service Level Reporting (SLR)	Over de IT-diensten van derden wordt gerapporteerd. De rapportage wordt geëvalueerd op het voldoen aan de gemaakte prestatie-afspraken.
5	**Continuïteit, backup en recovery**	
5.1	Continuïteitsplannen	Procedures en plannen zijn vastgesteld en gedocumenteerd.
5.2	Back-up	Het back-up-proces is ingericht en back-ups worden periodiek uitgevoerd.
5.3	Recovery	Periodiek worden restore-testen uitgevoerd voor de back-ups.
5.4	Uitwijk naar andere locatie	Een uitwijklocatie is aanwezig en het uitwijkproces is getest.
5.5	Robuustheid DDoS	Maatregelen zijn ingericht om een DDoS-aanval te kunnen weerstaan.

Bijlage D Lijst van afkortingen

Afkorting	Toelichting
AD	Active Directory, Microsoft
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BBN	Basisbeveiligingsniveau conform de BIO
BIO	Baseline Informatiebeveiliging Overheid
CDN	Content Delivery Network
DDoS	Distributed Denial of Service
CIBG	Agentschap Centraal Informatiepunt Beroepen Gezondheidszorg, ministerie van VWS
CISO	Chief Information Security Officer
CMDB	Configuration Management Data Base
COVA	Covid-19 Acceptatie-omgeving (ACC)
COVP	Covid-19 Productie-omgeving (PROD)
CSPO	Chief Security & Privacy Operations
CSR	Certificate Signing Request
DMZ	Demilitarized Zone. Dit is een nul-netwerk met een binnen-firewall en een buiten-firewall, om te zorgen voor isolatie tussen netwerken.
DPIA	Data Protection Impact Analyse (identiek aan GEB)
ELK	ElasticSearch, Kibana, Beats, and Logstash
FG	Functionaris voor de Gegevensbescherming
FMEA	Failure Mode Effects Analysis
GEB	Gegevensbeschermingseffectbeoordeling (identiek aan DPIA)
GGD	Gemeentelijke Gezondheidsdienst
HSM	Hardware Security Module
ICT	Informatie en Communicatie Technologie
IDS	Intrusion Detection System
IDU	Instroom, Doorstroom en Uitstroom
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAE	International Standard on Assurance Engagements
ITGC	IT General Controls
Justid	Justitiële Informatiedienst, Ministerie van Justitie en Veiligheid
KSP	KPN Security Policy
NAT	Network Address Translation
NIB	Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie
OTAP	Ontwikkel, Test, Acceptatie en Productie
OU	Organisation Units binnen de Active Directory (AD)
PKI	Public Key Infrastructure
RAID	Risks, Actions, Issues and Decisions
RCA	Root Cause Analysis
SLA	Service Level Agreements

Afkorting	Toelichting
SLR	Service Level Reporting
SIEM	Security Information & Event Monitoring
SOC	Security Operating Center
SSL	Secure Sockets Layer
TFA	Two Factor Authentication
TLS	Transport Layer Security
UPS	Uninterruptable Power Supply
VIR-BI	Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie
VPN	Virtual Private Network. Dit is een versleutelde verbinding over internet.
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
Wbni	Wet beveiliging netwerk- en informatiesystemen