Ministerie van Volksgezondheid,
Welzijn en Sport

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34

www.rijksoverheid.nl

Inlichtingen bij
5.1.2e

5.1.2e @minbzk.nl

memo

Datum
29 januari 2021

Aantal pagina's
4

Voorstel "De basis op orde in de Test- en Traceerketen"

Aanleiding/probleemstelling

Naar aanleiding van de actuele situatie rondom onder meer databeveiliging, cybercriminaliteit en de processen ten behoeve van de Covid-19 bestrijding, is de regiegroep DOTT door voorzitter LCT gevraagd om de hoogste prioriteit te geven aan een verbeterplan op deze punten. Onderstaand een verkort voorstel voor een stappenplan om de meest urgente zaken met betrekking tot informatieveiligheid en privacy in een versneld traject op te pakken. Dit met als uitgangspunt dat het aansluit op de uiteindelijke ketenoplossing en daarmee een stevig fundament vormt om daartoe te komen.
Kern van de verbetering zit in de digitale ondersteuning van de test- en traceerketen in het algemeen en die bij de GGD in het bijzonder. Dit om datalekken te voorkomen dan wel zo snel mogelijk op te lossen, en om informatie-uitwisseling betrouwbaar en snel te laten verlopen in de test- en traceerketen.

BeslispuntBeslispunt

LCT wordt gevraagd akkoord[1] te gaan met onderstaand verbeterplan, zodat dit versneld kan worden uitgevoerd.

Advies/actie

Het voorstel Basis op Orde bevat de volgende onderwerpen:

1. ICT landschap herijken en herinrichten (de techniek)
2. Informatiebeveiliging en privacy (de beveiliging/mens)
3. Informatieuitwisseling in de keten (de informatie/data-deling)

Doel is om op korte termijn in control te komen in de test-en traceerketen, om vervolgens de keten duurzaam te versterken voor de toekomst.

Deze onderwerpen komen terug in het portfolio, zoals dat in de maak is in de Werkgroep Follow-up Risicoanalyse (werktitel). Dit portfolio bestaat uit een breed scala aan onderwerpen die de komende tijd nader geprioriteerd zullen worden. De actuele conceptversie van het portfolio is opgenomen als bijlage.

[1] Conform opdrachtformulering Regiegroep DOTT worden adviezen en beslispunten voorgelegd aan LCT

Betrokken VWS-onderdelen
Staf Regiegroep DOTT, DI/RDO, pdC19

Toelichting
De urgentie is groot, prioriteit is aan een aantal basisvoorwaarden te voldoen. Hiermee wordt een fundament gelegd, waarna de test- en traceerketens verder kunnen worden geprofessionaliseerd, met stabiele en voorspelbare ketens als gevolg. De urgentie geldt ketenbreed, te beginnen met GGD (en GGD GHOR), RIVM en VWS. Later uit te breiden met laboratoria en andere ketenpartners.

Ad 1 ICT landschap herijken en herinrichten

Om het ICT landschap in control te krijgen, zijn de volgende actielijnen noodzakelijk:
- Heroverweging van systemen, waaronder het terugbrengen/terugschalen naar hun oorspronkelijke doel (zoals HP zone);
- Nieuwe systemen een logische plek geven, met afgebakende doelbinding
- Zorgen dat bij terugschaling van systemen de impact in de keten minimaal is en de continuïteit van de processen gewaarborgd (zoals bij ontvlechting van het BCO proces)
- Uitwerking hoe de nieuwe oplossingsrichtingen voldoen aan Rijksnormen, BIO compliant[2]
- Invoering van ketenbrede afspraken, zoals Life Cycle Management (LCM) om o.a. te zorgen dat alle omgevingen bijgewerkt zijn met vereiste patch en/of software release en zodoende minimaal kwetsbaar zijn voor aanvallen.
- Continue right-to-audit invoeren: afspraken hoe we samenwerken, vastgelegd in contracten moeten te allen te tijde getoetst kunnen worden door een door de opdrachtgever/ketenpartner aan te wijzen partij.

Ad 2 Informatiebeveiliging en privacy

Uitgangspunten op het gebied van informatiebeveiliging en privacy borgen:
- Security en privacy by design
- Bij toegang als stelregel "nee, tenzij" hanteren
- Herijking en verbetering van Autorisatie en Authenticatie, dwz ook in de werkprocessen en beheer zoals Identity & Access Management[3]
- Certificering van nieuwe oplossing
- Security en privacy onderdeel van contracten met leveranciers, incl. right-to-audit en sancties
- PDCA invoeren, periodiek risicoanalyse uitvoeren/herijken, dus ook bv vulnerability management inregelen voor ketenonderdelen
- Onafhankelijk auditor betrekken voor externe toetsing
- Voldoen aan NEN 7510; het doen van een ketenbrede nulmeting, gevolgd door een actieplan met noodzakelijke verbeteringen; inventariseren van noodzakelijke rollen en het doen van voorstellen voor specifieke autorisaties voor deze rollen. Hierbij verdient het aanbeveling zeer terughoudend om te gaan met toegang tot (medische) persoonsgegevens

---

[2] uitwerking van de eisen en kaders waar de nieuwe oplossingsrichting aan moet voldoen o.a. NEN 7510, Rijksnormen, BIO en AVG compliant (i.s.m. DI/RDO)

[3] Goed beheer van authenticatie en autorisatie helpt met het verlenen van de juiste toegang, niet teveel, niet te weinig, aan de juiste personen – en daarnaast met het direct intrekken van deze toegang, zelfs geautomatiseerd als dat moet.

- Robuuste omgeving, door sturen op gelaagde weerbaarheid (layered defense). Zodat het falen van 1 maatregel niet leidt tot falen van de keten.
- Compliancy: aantoonbaar voldoen aan actuele normen, onder meer zorgdragen dat alle betrokken omgevingen AVG en BIO compliant zijn.

Ad 3 Informatieuitwisseling in de keten borgen

Informatieuitwisseling in de keten moet geborgd blijven
- Incidentmanagement ketenbreed uitrollen
- Keteninformatievoorziening moet gecontinueerd blijven bij ontvlechting van het BCO proces
- Hygiëne in gegevensoverdracht tussen verschillende organisaties in de keten. Voortbordurend op de risico-analyse van december 2020: is van alle gegevensoverdrachten bij verzender en ontvanger bekend:
    a. Wat de inhoud is;
    b. Wat doel van de overdracht is;
    c. Hoe de security van de overdracht is geborgd;

En hierop te formuleren knelpunten en verbeterpunten identificeren.

BIJLAGE – CONCEPT PORTFOLIO DOTT

Digitale Ondersteuning Testen & Traceren (DOTT)
Planning op hoofdlijnen (concept)
29 januari 2021

NTB | IN PLANNING | OPGELEVERD | RISICO

Omschrijving	2021				2022
	1e kwartaal	2e kwartaal	3e kwartaal	4e kwartaal	1e kwartaal
Maatregelen met een hoge prioriteit en urgentie					
- Uitfaseren HPZone	Start onderzoek uitfaseren legacy software				
- Inrichten en uitrollen RBAC	Start met rollen gebaseerde toegangscontrole				
- Beperken van dataloogang	Compartimenteren				
- (Keten)Incidentmanagement inregelen	Verbeteringen oplossen				
- Informatie-uitwisseling in de keten borgen	Opstellen data-uitwisselingsovereenkomst				
- Implementeren server hardening	Onnodige zaken als usb poorten, export functies, servervrollen etc. zo veel mogelijk uitschakelen				
Korte termijn maatregelen (Quick Wins)					
- Quick Win tafel	Inrichten QW tafel	Regie en opvolging urgente issues			
- Verbeterplan Testen & Traceren	Opstellen Plan van Aanpak				
- Ketenbesturing	Inrichten ketenstrategie en -organisatie				
- Ketenvisie	Blauwdruk, missie en doelstellingen				
- Transitieplan	GAP analyse + Plateau planning				
- Keten Start Architectuur (KSA)	ICT landschap herijken en herinrichten				
- Informatiebeveiliging & Privacy	IB & Privacy duurzaam inregelen: security be design, autorisatie & authenticatie, certificering, voldoen aan (wettelijke) kaders etc.				
- Life Cycle Management (LCM)	Onderzoek uitfaseren legacy (o.a. HPZone)	LCM proces inrichten			
- Kwaliteits- & Risicomanagement	Kwaliteits- & Risicomanagement inrichten				
- Incidentmanagement	Incidentmanagement plan + verbetervoorstellen	<Incidentmanagement duurzaam inregelen>			
Lange termijn maatregelen (Duurzame oplossingen)					
- ICT dienstverlening in de keten	Ketendienstverlening				
- Gemeenschappelijk ethisch/ juridisch kader	Juridisch/ ethisch kader				
- Optimaliseren ketenprocessen (en koppelvlakken)	Optimaliseren ketenprocessen				
- Opslag, beheer en uitwisselen Test- & Traceerinformatie	Strategie t.a.v. Opslag, beheer en uitwisselen van Test- & Traceerinformatie				
- Robuust en schaalbaar BCO informatiesysteem	Essen en weinigen in kaart brengen + Meldplicht verruimen (o.a. Het WMO initiatief)				
Innovatie (Dromen)					
- Hergebruik data voor wetenschappelijk onderzoek	- Een robuuste en schaalbare (basis) ICT infrastructuur				
- Best practices and Lessons learned andere landen	- Noodprocedures/ calamiteitenplan bij pandemieen				
- Real-time informatie in Dashboard VWS					
- Self-service medisch dossier	- Meer internationale samenwerking op gebied van ICT (o.a. EU app testbewijzen, vaccinatiepaspoort)				
- Testinformatie centraal vastleggen					
- Geen regionale grenzen bij (nationale) crisis	- IT expertise aan tafel bij beleidsbeslissingen				