

FOD VOLKSGEZONDHEID
VEILIGHEID VAN DE VOEDSELKETEN
EN LEEFMILIEU

Brussel, 08/02/2024

Directoraat-generaal Gezondheidszorg

FEDERALE RAAD VOOR
ZIEKENHUISVOORZIENINGEN

Kenm.: FRZV/D/600-1 (*)

Advies van de FRZV - Cyber Security

Namens de voorzitter van de FRZV,
Margot Cloet,

Sabine Stordeur
Directrice-generaal

(*) Dit advies werd goedgekeurd door de plenaire op 08/02/2024 en door het Bureau op hetzelfde datum geratificeerd.

De FRZV wenst hierbij zijn advies kenbaar te maken als antwoord op de adviesvragen van minister Vandenbroucke dd. 5 december 2023 en 24 januari 2024 inzake het Cyber Programma.

1. Situering van de vraagstelling

De minister bevestigt in zijn adviesvraag van 24 januari het belang van adequate maatregelen inzake cyberveiligheid in de ziekenhuizen. Hij vermeldt daarbij de ondersteuning die de overheid voorziet voor het uitrollen van deze maatregelen sinds 2021. Waar de financiering tot dusver enkel naar de ziekenhuizen ging komen we nu in een nieuwe situatie waarbij met de uitrol van het Cyber Programma een gedeelte van het budget zal worden aangewend voor collectieve maatregelen. Ook de FRZV deed in het advies van 16 december 2021¹ reeds een aantal voorstellen voor collectieve initiatieven en is dus in globa positief over deze stap. De FRZV kan ook de doelstellingen van het Cyber Programma zoals opgesomd in de adviesvraag onderschrijven. Naast het optrekken van het niveau van cyber veiligheid en het creëren van een platform voor samenwerking is het inderdaad van uitzonderlijk belang de autonomie van het ziekenhuis in deze te blijven erkennen. Cyberveiligheidsrisico's zijn immers dezelfde voor elk ziekenhuis, maar de blootstelling aan deze risico's verschilt van ziekenhuis tot ziekenhuis volgens maturiteitsniveau en de ingevoerde beschermingsmaatregelen die het heeft genomen.

2. Ondersteuningsmechanisme Cyber Programma en voorwaarden

Lopende kosten en nieuwe initiatieven

Vooreerst zijn we verrast dat de minister in het nieuwe voorgestelde financieringsmechanisme afstapt van de tot dusver gehanteerde verdeelsleutel. De FRZV stelt voor deze, in tegenstelling tot het nieuwe voorstel waarbij de financiering proportioneel berekend wordt louter via het aantal bedden, te behouden. Een groot aantal van de kosten zijn immers moeilijk schaalbaar, wat – na de eerste verdeling tussen AZ (85,5%) en PZ (14,5%) – een verdeling van 50% per ziekenhuis (éénzelfde bedrag per ziekenhuis) en 50% proportioneel aan het aantal verantwoorde/erkende² bedden rechtvaardigt.

De minister stelt in zijn adviesvraag vast dat een aantal ziekenhuizen de ondersteuning tot dusver gebruikt heeft om de bestaande uitgaven voor cyberveiligheid te dekken. De bedoeling is echter om met de ter beschikking gestelde middelen nieuwe initiatieven te ontwikkelen die de cyberveiligheid bevorderen. Echter wensen wij in de eerste plaats begrip te vragen voor deze ziekenhuizen gezien de huidige financiële positie waarin nagenoeg de hele sector zich bevindt. Daarnaast moeten we ook stellen dat het niet mogelijk is om enkel nieuwe acties te financieren. De voorgaande acties, zeker als het gaat om aanpassingen aan software of infrastructuur, brengen doorgaans terugkerende kosten met zich mee zonder dat daar extra middelen tegenover staan. Het enkel financieren van nieuwe acties leidt bijgevolg tot een (verdere) kostenontsporing en is dus niet wenselijk. Het zal zaak zijn hierin een goede balans te vinden en we vragen dan ook dat men hiermee rekening houdt bij de beoordeling van de opgevraagde roadmaps. Overigens vestigen we de aandacht van de minister nogmaals erop dat de geormerkte budgetten allerminst tegemoetkomen aan de behoeften en dat zij hooguit 10 % van de

¹ <https://overlegorganen.gezondheid.belgie.be/nl/documenten/frzvd544-1-advies-van-de-frzv-betreffende-cybersecurity-deel-2>

² verantwoorde bedden + erkende bedden voor die bedindexen waarvoor geen verantwoorde bedden worden berekend, en voor de ziekenhuizen als bedoeld in artikel 33, §§ 1 en 2.

werkelijk gemaakte kosten dekken. De maatregelen op het gebied van cyberbeveiliging zijn zeker nodig maar worden steeds talrijker en het zijn zeer dure maatregelen. Aangezien zij niet worden gefinancierd, betekent dit de facto dat de ziekenhuizen verplicht zijn ze met eigen middelen te bekostigen. We weten echter allen hoe het staat met die eigen middelen.

Afbouw van individuele ondersteuning

Het budget zou de komende jaren verdeeld worden tussen de ziekenhuizen individueel, collectieve trajecten en accelerator ziekenhuizen. Daarbij valt op dat het individueel budget significant afneemt in de tijd, tot 40% vanaf juli 2027. Hierbij zijn twee kanttekeningen te maken. Eerst en vooral moet er nog voldoende budgettaire ruimte zijn voor het ziekenhuis om de voorziene autonomie voldoende op te nemen en context specifieke maatregelen te nemen. Daarnaast moet de meerwaarde van de collectieve maatregelen voor de ziekenhuizen minstens even groot zijn als het bedrag dat wordt afgestaan aan het collectief. Zo zal ten opzichte van 2023 in 2024 de individuele financiering per ziekenhuis 14% lager uitvallen. Wil men evenveel realiseren in 2024 dan in het voorgaande jaar dan zal dit enkel mogelijk zijn door zeer effectieve collectieve maatregelen. Hoe groter het collectieve budget, hoe groter de impact zal moeten zijn van deze collectieve maatregelen voor de individuele ziekenhuizen. De FRZV vraagt dan ook dat men niet zou uitgaan van een vooraf gedefinieerd traject van budgettaire collectivering, maar dat men op basis van de in het lopende jaar gerealiseerde collectieve trajecten en de realistisch te voorziene trajecten in de nabije toekomst het aandeel aan collectieve middelen voor het volgende jaar zou bepalen in samenspraak met de ziekenhuizen (zie verder voor governance aspecten). In deze benadering vervalt bijgevolg de voorgestelde verdelingstabel en wordt voor het bepalen van het budget voor 2024 en volgende een inschatting gemaakt binnen de voorziene governance structuren, waar de ziekenhuizen deel van uitmaken. Eén van de te voorziene trajecten houdt een goede samenwerking in met het federale CERT (Cyber Emergency Response Team van het CCB). Bovendien moet men de oprichting van een specifieke CSIRT (Computer Security Incident Response Team) voor de gezondheidssector overwegen. Dit team moet beschikbaar zijn voor alle ziekenhuizen die de behoefte uiten, mits enkele fundamentele praktijken worden gerespecteerd die nodig zijn voor een effectieve tussenkomst van een CSIRT.

(Sectorbrede) effectiviteit van collectieve maatregelen

Het verschuiven van het budget naar collectieve maatregelen wil zeggen dat men de collectieve middelen tijdig kan aanwenden en dat de meerwaarde die men realiseert niet al te zeer verschilt over de ziekenhuizen. Zo niet ontnemt men een aantal ziekenhuizen middelen die beter individueel zouden besteed zijn of anders gezegd zou het cyberrisico bij deze ziekenhuizen niet optimaal kunnen worden afgedekt gegeven de beschikbare middelen. Het is natuurlijk belangrijk daar in te grijpen waar de nood het hoogst is, maar men mag de ziekenhuizen die op dit vlak voorsprong hebben genomen niet penaliseren.

Accelerator

Integendeel, men verwacht van deze ziekenhuizen dat zij een leidende rol opnemen en dat zij inzichten en goede praktijken delen ten bate van de gehele sector. Hiervoor wordt een accelerator financiering voorzien. Echter, de voorwaarden waaraan een ziekenhuis moet voldoen om in aanmerking te komen voor deze financiering zijn onduidelijk. Bovendien is het nut van dergelijke inzichten en goede praktijken afhankelijk van de onderwerpen die op een bepaald moment collectief bekeken worden. Om te vermijden dat veel ziekenhuizen zich als accelerator zouden aanmelden, ten andere een vrij vaag begrip in deze, en aldus de financiële prikkel te niet zou worden gedaan stellen wij voor het delen van expertise en goede praktijken anders te vergoeden, namelijk uit het collectief budget, volgens de noden die het collectief op dat moment ondervindt. Op die manier kan het collectief significante

inspanningen van individuele ziekenhuizen ten behoeve van het collectief vergoeden, waardoor deze ziekenhuizen sneller de nodige expertise kunnen vrijmaken. Concreet stellen we dus voor het accelerator budget te schrappen en dit budget opnieuw toe te voegen aan het individueel budget. De voorgestelde werkwijze zal immers veel kostenefficiënter zijn doordat ze enkel gaan naar ziekenhuizen die een significante inspanning leveren die zonder vergoeding niet mogelijk is, bijvoorbeeld het ter beschikking stellen van bij hen tewerkgestelde experts. De resterende budgetten kunnen dan best naar alle individuele ziekenhuizen gaan in plaats van naar de ongetwijfeld ruime groep van ziekenhuizen die zich als accelerator zou aanmelden, mede gezien de vage omschrijving van het begrip accelerator. Wij benadrukken de noodzaak om de ziekenhuizen daadwerkelijk te vergoeden voor de deskundigen die zij ter beschikking stellen wanneer hun expertise wordt ingeroepen. De ziekenhuizen beschikken immers over zeer beperkte menselijke en geldelijke middelen en iedere vraag om vaardigheden te delen moet financieel worden gecompenseerd, wil men dit initiatief werkelijk kans op slagen geven. De FRZV benadrukt ook dat men de ziekenhuizen tijdig moet informeren (voldoende tijd geven) als men ze vraagt hun deskundigen ter beschikking te stellen, opdat zij hieraan zouden kunnen deelnemen.

Governance

Het is voor de doelmatigheid van de inzet van het budget van uitzonderlijk belang dat de ziekenhuizen kunnen deelnemen aan de beslissingen over het bepalen van het collectief budget, de aanwending ervan en de controle op de uitvoering van de collectieve maatregelen. Daarom vraagt de FRZV dat de ziekenhuizen een afdoende vertegenwoordiging zouden krijgen in het SteerCo.

Globaal Budget en NIS2

Verder wenst de FRZV met respect op te merken dat het ter beschikking gestelde budget substantieel is, maar niet voldoende om met de gehele sector een afdoende maturiteitsniveau te bereiken. In het kader van de budgetbesprekingen is reeds meegedeeld dat een structureel budget van 130 mio euro nodig is en daarbovenop nog 40 mio euro voor de bijkomende ingrepen in het kader van de NIS2 regelgeving.

Timing

Tot slot vraagt de FRZV om de deadline van 15/3 (of zelfs 31/3³) om de benodigde vragenlijsten, documenten en rapporten⁴ in te vullen en terug te sturen minimum uit te stellen naar 31/5/2024 gezien de ziekenhuizen tot heden niet geïnformeerd werden over de inhoud ervan. Als de betaling van 1/7 niet in het gedrang mag komen, voorziet men best een vereenvoudigde vragenlijst.

³ Zie adviesvraag 5/12/2023

⁴ Zowel het „*verslag met stand van zaken over de gedane cyberinvesteringen, en de verwachte effecten van die investeringen*” als de „*beschrijving van haar cybersecurity governance (rollen en belangrijkste verantwoordelijkheden, besluitvormingsmechanismen en beslissingsketens, en, indien van toepassing, de voornaamste comités), prioritaire cyberthema’s en geïdentificeerde aankomende cyberprojecten (roadmap)*”, zonder te spreken van het „*self-assessment maturiteitsniveau*» dat later nog moet worden voorzien.