FOD VOLKSGEZONDHEID
VEILIGHEID VAN DE VOEDSELKETEN
EN LEEFMILIEU

Directoraat-generaal Gezondheidszorg

FEDERALE RAAD VOOR
ZIEKENHUISVOORZIENINGEN

Brussel, 29 juni 2021

Kenm.: FRZV/D/536-2 (*)

Advies van de FRZV op de vraag van minister Vandenbroucke d.d. 19/05/2021 betreffende BMUC en Cybersecurity

Namens de Voorzitter,
Margot Cloet

Annick Poncé
directeur-generaal ad interim

Isabelle Van der Brempt (Signature)
Digitally signed by Isabelle Van der Brempt (Signature)
Date: 2021.07.07 23:00:32 +02'00'

(*) Dit advies werd goedgekeurd (via mail) door de plenaire op 29/06/2021 en op dezelfde datum door het Bureau geratificeerd.

De FRZV wenst met dit advies een antwoord te geven op de vraag van minister Vandenbroucke in zijn adviesaanvraag dd. 19/05/2021 betreffende BMUC en Cybersecurity.

Voorafgaand wil de FRZV beklemtonen dat het uitgebrachte advies zowel betrekking heeft op de Algemene Ziekenhuizen als de Psychiatrische ziekenhuizen

Procedure

In aansluiting op deze adviesvraag werden in de schoot van de FRZV twee werkgroepen opgericht om zich over deze adviesvraag uit te spreken.

In eerste instantie werd een werkgroep BMUC opgericht, bestaande uit leden van de FRZV en aangevuld met de nodige experten van de sector. Er werd beslist binnen de werkgroep, mede op vraag van de minister, om voor 1 juli een advies uit te brengen betreffende de BMUC-financiering voor het jaar 2022. Het doel is om op deze manier advies te kunnen verstrekken over de korte termijn doelstellingen 2022 betreffende de financiering van het EPD in de ziekenhuizen op basis van de BMUC-criteria. Aansluitend zal deze werkgroep zich dan verder buigen over de modaliteiten voor 2023 tem 2024, uitgaand van de context en de nagestreefde speerpunten in de verdere aanpak zoals deze in de advies geformuleerd worden.

Daarnaast werd een tweede werkgroep opgericht met als onderwerp Cybersecurity. Ook hiervoor werd een mix van leden van de FRZV en experten uit de sector bij elkaar gebracht. Zoals gesteld in de adviesvraag van de minister ligt de focus van het advies op de prioritaire speerpunten die vermeld worden: het creëren van awareness en het formuleren van een beleid om de maturiteit van de cybersecurity in de ziekenhuizen te vergroten. De werkgroep wil tevens de belangrijkste kosten verbonden aan de uitbouw van cybersecurity in de ziekenhuizen in kaart brengen. In het advies wordt verwezen naar een nieuwe Europese directieve met betrekking tot de beveiliging van netwerk- en informatiesystemen. Ook deze werkgroep zal zich aansluitend buigen over de modaliteiten voor de komende jaren, hierbij uitgaande van de prioriteiten die in de adviesvraag worden aangegeven.

Advies omtrent de financiering van het EPD via het BFM 2022

Situering

Sinds maart 2020 en tot op heden worden de ziekenhuizen geconfronteerd met de COVID-19 pandemie. Quasi de volledige aandacht van de ziekenhuissector wordt in beslag genomen door de noodzakelijke maatregelen om deze pandemie onder controle te brengen. Hierdoor is de ruimte in de ziekenhuizen om op een gestructureerde en gecoördineerde wijze de verdere ontplooiing van het EPD en de toetsing via de BMUC-criteria zeer beperkt geweest. De FRZV is er zich van bewust dat het reeds het tweede jaar op rij is dat op basis van de heersende pandemie de snelheid van de evolutie van de uitrol van het EPD vertraagt.

Het introduceren van nieuwe criteria in de opvolging van de evolutie van de uitrol van het EPD om op basis hiervan de financiering in het BFM 2022 te kunnen bepalen, het vastleggen van de normwaarden die bereikt dienen te worden, de omzetting in concrete acties in de ziekenhuizen en ten slotte ook de noodzakelijke metingen om de verwezenlijkingen te kunnen objectiveren, zijn dan ook moeilijk haalbaar.

Voorstel tot advies

In 2020 werden door de FRZV twee adviezen over deze aangelegenheid uitgebracht. Een eerste advies over de financiering in het BFM 1 juli 2020 (FRZV/D/507-3 – goedgekeurd door de plenaire vergadering van de FRZV op 23/04/2020). En een tweede advies over de financiering in het BFM van 1 juli 2021 (FRZV/D/522) goedgekeurd door de plenaire vergadering op 10/12/2020).

De FRZV stelt voor om deze adviezen te hernemen en onveranderd toe te passen in de financiering 2022. Meer bepaald adviseert de FRZV over de financiering van het EPD in het kader van het BFM van juli 2022, om de financieringsmodaliteiten van 2020 en 2021 te verlengen met 1 jaar en dus in 2022 op dezelfde manier de financiering te berekenen als in 2020 en 2021

Verdere aanpak

De werkgroep BMUC engageert zich evenwel om in juli 2021 een agenda op te stellen voor verdere aanpak met betrekking tot de financieringsjaren 2023 en 2024. Hierbij zullen de in de adviesvraag aangebrachte speerpunten leidend zijn. Dit zal binnen de stapsgewijze benadering gekaderd worden zoals ook in de adviesvraag werd geformuleerd. De FRZV streeft er naar om hieromtrent een advies te verstrekken voor eind 2021 zodat tijdig de communicatie naar de ziekenhuizen kan gebeuren, de implementatie kan opgestart en uitgebouwd worden en de nodige metingen kunnen verricht worden binnen een redelijk tijdskader. Hierbij dient blijvende aandacht te gaan naar de reeds bestaande differentiatie van de criteria tussen de algemene en psychiatrische ziekenhuizen.

Advies omtrent Cybersecurity

Situering

De FRZV treedt de visie dat cyberveiligheid in de Belgische ziekenhuizen een prioriteit dient te zijn, volledig bij. Enkele recente incidenten hebben duidelijk gemaakt dat de gezondheidssector een doelwit vormt voor malafide handelingen met verstrekkende gevolgen. De enorme hoeveelheid aan data met een grote gevoeligheid, maken het noodzakelijk om zich zo goed mogelijk te beschermen tegen onheus gebruik van deze gegevens. De lessen die uit deze recente incidenten worden getrokken, zetten de ziekenhuizen aan om grondig na te denken over een gepast strategie om de problematiek van de cybersecurity aan te pakken. De aandacht voor deze problematiek die blijkt uit deze adviesvraag, met de belofte tot organisatorische en bestuurlijke ondersteuning vanuit de overheid, verheugt de FRZV. De FOD maakte tijdens de bijeenkomsten ook duidelijk dat in 2022 hiervoor een financiële vergoeding zou voorzien worden.

Prioritaire focus van de FRZV

Zoals aangegeven in de adviesvraag van de minister heeft de FRZV zich in een eerste advies gericht op de items: “Awareness creëren” en “Maturiteit mbt cybersecurity beleid vergroten”.

De FRZV heeft hierbij een traject willen uittekenen dat deze elementen in de aanpak van de cyberveiligheid op een logische manier opbouwt. Het richtsnoer dat voor deze benadering wordt gebruikt, zijn de Europese NIS-richtlijn en de ISO 27001 norm. Zoals aangegeven in de adviesvraag van de minister werkt Europa aan een nieuwe versie van de NIS Directieve. Deze is echter vandaag nog niet gekend en kan dus op dit ogenblik nog niet gebruikt wordt als leidend voor de voorgestelde aanpak. De FRZV baseert zich in eerste instantie op generieke overwegingen die in elk normenkader kunnen geïntegreerd worden. Daarnaast zal de FRZV geleidelijk de ontwikkelingen van de nieuwe versie van de NIS richtlijn in zijn overwegingen betrekken, met inbegrip van de gevolgen van de aanwijzing van

gezondheidsoperators als O.E.S. (Operators of Essential Services) (zie in dit verband de brief van De FRZV aan de minister ref. CFEH/C/41-2021, van 11/03/2021).

Voorstel van stappen in de opstart van een cultuur omtrent cybersecurity in de ziekenhuizen

- De FRZV stelt dat als eerste stap in de aanpak van de cybersecurity, een grondige interne evaluatie dient te gebeuren in elk individueel algemeen en psychiatrisch ziekenhuis. De startpositie van elk ziekenhuis kan zeer uiteenlopend zijn. Deze diversiteit heeft te maken met reeds ondernomen stappen in het verleden, de omvang van de interne ICT-dienst, reeds doorgevoerde investeringen, uitgetekende processen, … Kortom: vooraleer de beste aanpak in de volgende stappen kan beoordeeld worden, dient de huidige situatie grondig in kaart gebracht en geëvalueerd te worden.

- De FRZV pleit voor ~~een~~ het uitvoeren van een externe audit waar de conformiteit met de bestaande regels en de mate van bescherming wordt getoetst door een externe partij. Hierbij zijn meerdere invalshoeken qua aanpak mogelijk: het te toetsen kader, het al dan niet gebruik maken van pentesting, ethical hacking, … Audit door een externe partij om de situatie "as is" en de gap tegenover het normenkader vast te kunnen stellen. Hierbij dient wel opgemerkt te worden dat deze stap niet onmiddellijk leidt tot een verhoogde cyberveiligheid maar wel de tekortkomingen in het systeem kunnen aantonen. Eventueel kan hier gekozen worden voor het gericht auditen op basis van de recente bevraging door de overheid betreffende cybersecurity bij de ziekenhuizen. Een tweede belangrijk aandachtspunt is het repetitief karakter van sommige acties, zoals bv. ethical hacking om de beveiliging verder op te volgen. Gezien het evolutieve karakter van de bedreiging zal deze stap ook met een zekere regelmaat dienen herhaald te worden, bv. om de 3 jaar. De FRZV stelt voor om hierover de nodige afspraken te maken met Belac, de Belgische accreditatie-instelling

- Een volgende stap in het traject is om op basis van de bevindingen van de externe audit en eventuele aanvullende stappen, een plan op te stellen om de waargenomen tekortkomingen aan te pakken. Dit is opnieuw een stap die intern in de organisatie (al dan niet onder begeleiding van externe partners) dient gezet te worden. Een organisatiebreed veiligheidsbeleid dient uitgewerkt te worden, vanzelfsprekend met als doel beveiliging tegen interne én externe bedreigingen van het systeem.

- De FRZV stelt voor om de aanpak van de problematiek omtrent cybersecurity ook te toetsen aan ervaringen in het buitenland. Hierbij wordt verwezen naar de ervaringen die opgebouwd werden, bv. in Nederland of Frankrijk. [1]

- De FRZV neemt ook kennis van een risico-analyse die in het verleden reeds door de FOD Volksgezondheid werd uitgevoerd en inzage kan geven in de toestand in België. Deze

[1] Frankrijk heeft zopas zijn programma voorgesteld om ziekenhuizen te helpen met cyberveiligheid: 2 miljard voor de digitale transformatie van ziekenhuizen, waarvan **350 miljoen euro voor cyberveiligheid**. De 135 GHT's (groupements hospitaliers de territoire) worden officieel O.E.S. (https://www.patientnumerique.com/actus/actualites/2021/04/la-france-devoile-un-programme-dassistance-aux-hopitaux-en-matiere-de-cyber-securite/).

informatie kan gebruikt worden om meer gericht de behoeftes van de ziekenhuizen te detecteren en meer gericht op een overkoepelend niveau actiepunten te definiëren.

Creëren van awareness in de organisatie

De FRZV pleit voor een grondige aanpak in de ziekenhuizen om op alle niveau's in de organisatie en overal op de werkvloer, de nodige sensibilisering voor de problematiek én de noodzakelijke stappen die dienen gezet te worden om cybersecurity te borgen, door te voeren. De mogelijke bedreigingen voor de digitale systemen zijn divers en kunnen overal in een ziekenhuis optreden. Iedereen dient bijgevolg op de hoogte te zijn van deze potentiële risico's én de protocollen die hieromtrent worden afgesproken.

De opleidingen die hieromtrent dienen gegeven te worden, dienen aangepast te zijn aan de verschillende omstandigheden in functie en omgeving. Het is ook belangrijk dat ~~deze~~ sensibilisering en opleidingen regelmatig herhaald worden. Hiervoor kan beroep gedaan worden op permanente trainingstools en sensibiliseringsacties. De FRZV pleit voor het ontwikkelen van een e-learning programma bestaande uit verschillende modules.

Verzekerbaarheid van het risico

De FRZV stelt een specifieke problematiek vast omtrent de verzekerbaarheid van het risico op inbreuken op cyberveiligheid. De verzekeringsssector verhoogt de premies om dit soort risico's te dekken. Desgevraagd wordt hier verwezen dat dit een tendens is van de internationale markt. Het belang van het kunnen behouden van een betaalbare optie tot verzekerbaarheid wordt door de sector als zeer belangrijk ervaren. Hierbij wordt verwezen naar het inschakelen van hulp-teams bij een externe cyberaanval maar ook naar het dekken van eventuele financiële claims, niet alleen gekoppeld aan deze externe cyberaanval maar ook door eventuele tekortkomingen in de zorgverlening als gevolg van de gehele of gedeeltelijke uitval van systemen.

Kennisdeling

De FRZV wil benadrukken dat in deze belangrijke en delicate materie, het delen van kennis een zeer cruciaal punt is. Cybersecurity gaat niet om competitie tussen ziekenhuizen maar om een gezamenlijke houding t.o.v. een potentieel toxische agressie met als inzet de zorg- en gezondheidsdata van onze patiënten. Om die reden is het belangrijk dat de ziekenhuizen zich rond deze problematiek verenigen en zoveel mogelijk de kennis hieromtrent delen. Hierbij wordt gedacht aan een organisatiestructuur bijvoorbeeld op netwerkniveau om informatie te delen, maar aangezien de problematiek de netwerken overstijgt, dient dit op een veel breder platform bekeken te worden.

Er bestaan meerdere informele kanalen waar uitwisseling kan gebeuren maar het verder faciliteren van samenwerking, specifiek op het vlak van cybersecurity, wordt door de FRZV als een belangrijke taak van de overheid gezien. Uitwisseling van best-practices, maar ook het delen van actieplannen zijn belangrijke items. De FRZV zou hier ook pleiten voor participatie van vertegenwoordigers uit de nationale cel Cybersecurity om aan dit overkoepelend platform te participeren. Ten slotte wil de FRZV er ook op wijzen dat andere maatschappelijk belangrijke groepen met deze problematiek geconfronteerd worden (bv. politiediensten) en het uitwisselen van kennis dus wel een heel breed platform zou kunnen gebruiken.

Samenvattende elementen advies

- Traject in elke instelling: interne evaluatie, externe beoordeling, opstellen actieplan
    - Toetsen aan buitenlandse ervaringen
    - Terugkoppeling risico-analyse FOD Volksgezondheid in de sector
- Creëren awareness in de organisatie door opleiding en sensibilisering
- Verzekerbaarheid van de risico's
- Kennisdeling binnen de sector maar ook over de sectoren heen

Financiële aspecten cybersecurity

De FRZV neemt kennis van de mogelijkheid die in het vooruitzicht wordt gesteld om een financiering te voorzien ter ondersteuning van het ontplooien van een plan van aanpak Cybersecurity met concrete actiepunten in de ziekenhuizen. Het is dan ook belangrijk om in dit eerste advies omtrent cybersecurity een eerste aanzet te geven over de mogelijke kosten waarmee de ziekenhuizen in dit kader geconfronteerd worden.

Bestaande functies met toegevoegde waarde

Sinds mei 2018 dient elke organisatie te beschikken over een Data Protection Officer (DPO) bovenop de informatieveiligheidsadviseur. Deze functies en hun exploitatiekosten werden niet bijkomend vergoed vanuit de overheid. Ondertussen zijn de kennisvereisten en het takenpakket van deze functies, oa. door de introductie van de GDPR-regels, flink uitgebreid. Ook in het kader van de problematiek van cybersecurity en de noodzakelijke stappen die door de FRZV gedetecteerd werden om de awareness en de maturiteit van de organisatie te beoordelen, wordt het takenpakket van deze functies aanzienlijk uitgebreid. De FRZV wil dan ook pleiten dat vanuit de overheid deze functies en hun exploitatiekosten (op jaarbasis voor alle ziekenhuizen samen berekend op 37,5 miljoen euro[2]) mee worden genomen om een passende structurele financiering te voorzien. De positie van de DPO en de informatieveiligheidsadviseur in deze context is centraal en cruciaal. Het lijkt dan ook onaanvaardbaar dat deze belangrijke sleutelpositie in de coördinatie van de cybersecurity niet zou gecompenseerd worden.

Kosten verbonden aan het traject

- Het uitvoeren van de externe toetsing brengt extra kosten met zich mee. De FRZV stelt vast dat het kostenplaatje van een dergelijke externe toetsing varieert van ziekenhuis tot ziekenhuis en de inhoud van de externe toetsing. De bedragen variëren tussen 11.000 tot 80.000 euro voor een externe audit, 26.000 tot 150.000 euro voor een ISO27001 toetsing. Gezien dit een essentieel onderdeel is van het traject dat een ziekenhuis dient te lopen, zal dit zeker een vast onderdeel zijn, met een extra jaarlijks terugkerend onderdeel (onderhoud). Bovendien zorgt de installatie van een SIEM ("Security Information Event Management")/SOC ("Security Operations Center") voor een hoog niveau van cyberbeveiliging. De kost hiervan wordt ingeschat op minimum 50.000 euro per jaar per ziekenhuis. De FRZV stelt dan ook voor om op basis van verdere vergelijkende studie en een verdere concretisering van het traject een bedrag op te nemen in de financiële tegemoetkoming.

- De verzekerbaarheid van het risico verbonden aan cyberveiligheid is momenteel in te schatten op een bedrag tussen 40.000 en 180.000 euro. Ook hier is er variatie op basis van de grootte van de instelling en het te verzekeren risico. Gezien de FRZV de verzekerbaarheid van het risico

[2] Zie fiche 8 van advies FRZV/D/514-2 prioritaire behoeften 2021, van 9 juli 2020

als een zeer belangrijk element beschouwd, dient in de bepaling van de financiële tegemoetkoming dit nader bepaald te worden.

- Het creëren van de nodige awareness bij de medewerkers in de gehele organisatie dient te gebeuren via opleiding en regelmatige herhalingssessies. Om de financiële impact van een ziekenhuisbrede opleiding te duiden, geven we hierbij een voorbeeld. Voor een opleiding in klassikaal verband gedurende 2 uur van alle medewerkers in de organisatie wordt dit berekend op een totaalbedrag van 15 miljoen euro. Het is vooral de opportuniteitskost, meer bepaald de vervanging van zorgpersoneel wanneer ze de opleiding volgen, die zwaar doorweegt. Andere opleidingstrajecten zijn uiteraard ook mogelijk, bv. 10 min per maand een korte e-learning module doorlopen, weegt minder op de afwezigheid van zorgpersoneel, maar betekent op jaarbasis ook wel 2u "afwezigheid" per medewerker. De FRZV wil daarom benadrukken dat de vele "beetjes" die zorgpersoneel weghalen bij het bed samen ook zwaar doorwegen en een kost met zich meebrengen.

- De kennisdeling wordt als zeer belangrijk beschouwd door de FRZV. Naast de bestaande informele kanalen waar uitwisselen van ervaringen mogelijk is, vraagt de FRZV toch naar een meer overkoepelend platform vanuit de overheid waar ook in een breder maatschappelijk kader de nodige uitwisseling van ervaring en kennis kan gebeuren. De FRZV vraagt echter ook vanuit de overheid een ondersteuning van de initiatieven op meer lokaal niveau, bv. op netwerkniveau.

Manier van vergoeding

Wat betreft de verdeling van de beschikbare financiële middelen die beschikbaar zouden worden gesteld van de ziekenhuizen, heeft de FRZV geen objecties om dit analoog op te bouwen met de manier waarop de EPD-financiering gebeurt.

De opbouw van de financiering bestaat uit een sokkelfinanciering (bestaand uit een vast bedrag onafhankelijk van de grootte van het ziekenhuis en een bedrag per bed), een acceleratorfinanciering (ook bestaand uit een vast bedrag onafhankelijk van de grootte van het ziekenhuis en een bedrag per bed) en – eventueel en in beperkte maat - een kennisdelingsfinanciering. Hierbij wordt gestreefd naar een eenvoudig en transparant systeem. De financieringscriteria dienen ook tijdig te worden gecommuniceerd aan de ziekenhuizen.

Het is echter van belang dat in de beginfase (lancering van de aanpak) de sokkelfinanciering voldoende substantieel is om de eerste stappen die door de ziekenhuizen worden gezet, te ondersteunen. Na deze nodige booster moet het vervolgens mogelijk zijn de financieringsregelingen geleidelijk te verfijnen aan de hand van criteria.

Verder plan van aanpak

De werkgroep Cybersecurity zal in juli/september 2021 een plan van aanpak maken om het advies voor de verdere toekomst uit te werken, daarbij zich richtend op de speerpunten en prioriteiten die in de adviesvraag geformuleerd worden. Het doel is om voor het einde van 2021 een tweede advies voor te leggen omtrent de toekomstige aanpak van de cybersecurity.

***