FOD VOLKSGEZONDHEID
VEILIGHEID VAN DE VOEDSELKETEN
EN LEEFMILIEU

Directoraat-generaal Gezondheidszorg

FEDERALE RAAD VOOR
ZIEKENHUISVOORZIENINGEN

Brussel, 16 december 2021

Kenm.: FRZV/D/544-1 (*)

Advies betreffende cybersecurity – deel 2

Namens de Voorzitter,

Margot Cloet

Annick Poncé
(Signature)

Digitally signed by Annick Poncé
(Signature)
Date: 2022.01.11 10:44:18 +01'00'

Annick Poncé

directeur-generaal ad interim

(*) Dit advies werd goedgekeurd door de plenaire op 16/12/2021 en op dezelfde datum door het Bureau geratificeerd.

De FRZV wenst hierbij zijn advies kenbaar te maken als antwoord op de adviesvraag van minister Vandenbroucke van 19 mei 2021.

In een eerste advies FRZV/D/536-2(*) van 29 juni 2021 werd op enkele urgente vragen reeds een antwoord gegeven. Daarbij werd ook een eerste positionering beschreven t.a.v. de gestelde problematiek van Cybersecurity.

1. *Situering van de vraagstelling*

In de adviesvraag van 19 mei 2021 situeerde de minister de intentie om vanuit het kabinet de ziekenhuizen op organisatorisch en bestuurlijk vlak te ondersteunen bij de implementatie van het cybersecurity beleid, met nadruk op responsabilisering en het borgen van de doelstellingen op lange termijn. Ook werd verwezen naar de nodige voorbereidingen op het verschijnen van een nieuwe Europese Richtlijn betreffende deze materie. De nadruk zal hierbij liggen op het risicobeheer en het zich conformeren met een lijst van minimale veiligheidsingrepen.

Ondertussen werd in de schoot van de FRZV een werkgroep van experten opgericht die zich buigt over deze problematiek.

Er werd in de adviesvraag ook bijzondere aandacht gevraagd voor het creëren van awareness in de sector en de doelstelling om de maturiteit m.b.t. het security beleid te vergroten.

2. *Voorafgaande bemerkingen*

Op de gezamenlijke vergadering van de werkgroep BMUC en Cybersecurity van 17 november 2021, werd door het kabinet toelichting gegeven bij de voorziene budgetten voor o.a. het luik Cybersecurity. De FRZV werd hierbij op de hoogte gesteld dat voor het jaar 2022 een bedrag van **20 miljoen euro** ter beschikking van de ziekenhuizen is. Het zou gaan om een **éénmalige** input van financiële middelen. De FRZV is erkentelijk voor de input van deze financiële middelen als noodzakelijke ondersteuning om een belangrijke bedreiging van onze gezondheidszorg te kunnen aanpakken. Anderzijds betreurt de FRZV dat het gaat om een éénmalige budget. Het is immers zonder meer duidelijk dat de bedreiging die uitgaat van cyberaanvallen meer en meer een chronisch karakter kent met vaak verstrekkende gevolgen die niet op te lossen zijn door éénmalig in mensen en middelen te investeren.

De FRZV verwijst ook naar een recente bevraging bij de Vlaamse ziekenhuizen naar de **kostprijs** per bed van de noodzakelijke inspanningen op het vlak van cybersecurity. Hierbij werd vastgesteld dat de gemiddelde kostprijs per bed is opgelopen van 368 euro per bed in 2019 tot 484 euro per bed in 2020. Op basis van deze cijfers komt men aan een jaarlijkse kost van meer dan 24 miljoen euro voor alle algemene en psychiatrische ziekenhuizen in België samen. Het aanpassen van het maturiteitsniveau aan het huidige en toekomstige dreigingsniveau zal dus een structurele financiering vergen. Een ontoereikende financiering zal het systemische cyber-risico stelselmatig vergroten, terwijl zich nu reeds een aantal ziekenhuizen in de gevarenzone bevindt.

De FRZV stelt immers vast dat er in het afgelopen jaar tot op heden 3 majeure cyberaanvallen hebben plaatsgevonden op ziekenhuizen met verstrekkende gevolgen op de dienstverlening en mogelijke implicaties op de kwaliteit van zorg. Het gaat dus niet langer om incidentele gebeurtenissen, maar het toont aan dat de zorgsector in het algemeen (en de ziekenhuizen in het bijzonder) een **gericht doelwit** vormen voor dit soort van aanvallen. Ook informatie vanuit internationale context wijst op deze tendens.

De FRZV stelt vast dat de stappen die tot op heden door de ziekenhuizen zijn gezet in de aanpak van deze problematiek, **sterk uiteenlopend** zijn. Er zijn ziekenhuizen die al verregaand ingezet hebben op de evaluatie en aanpassing van hun systemen. Andere ziekenhuizen zijn momenteel nog in de opstartfase. Wanneer we in het verdere advies omtrent de voorgestelde aanpak van cybersecurity in de ziekenhuizen verder in detail omschrijven welke stappen moeten gezet worden, dient de minister er rekening mee te houden dat sommige stappen in een aantal ziekenhuizen al gezet zijn, terwijl deze voor andere de basis zullen vormen van hun verdere aanpak. De FRZV wil erop wijzen dat in de finaliteit van bescherming tegen cyberattacks het vanzelfsprekend is dat er best gestreefd wordt naar een proactieve benadering waarbij potentiële aanvallen tijdig gedetecteerd en afgewend worden. Alle andere maateregelen zijn secundair, maar daarom niet minder belangrijk. We zullen deze verschillende elementen dan ook als dusdanig benaderen.

Ten slotte wil de FRZV voorafgaandelijk nog benadrukken dat de financiering bij voorkeur **op het niveau van het individuele ziekenhuis** wordt toegekend. Zoals hoger reeds vermeld, is er een brede range van maturiteit in de ziekenhuizen wat betreft cybersecurity. Dit betekent dat elk ziekenhuis met eigen prioriteiten geconfronteerd wordt die een eigen invulling noodzakelijk maken. Dit wil niet zeggen dat er geen aandacht moet zijn voor collectieve oplossingen. Waar mogelijk moet gekeken worden waar men tot onderlinge samenwerking kan komen voor een zo efficiënt mogelijke besteding van de middelen (zie ook verder).

3. *Cyber security acties in de ziekenhuizen*

De FRZV wil hierbij graag verwijzen naar het advies FRZV/D/536-2(*) waar reeds in detail werd ingegaan op de te ondernemen stappen en de financiële implicaties.

Graag willen we hier nogmaals de verschillende stappen onder de aandacht brengen, evenwel rekening houdend met de voorafgaande vaststellingen dat een aantal van deze stappen reeds werden gezet door sommige ziekenhuizen. Daarom is de FRZV ook geen voorstander om een aantal van deze stappen te verplichten. Het verplicht hernemen ervan (bv. een sectorbrede audit) is geen efficiënte besteding van de schaarse middelen of, anders gezegd, het gaat om middelen die ziekenhuizen op een veel betere manier kunnen aanwenden in maatregelen die een hogere graad aan bescherming opleveren.

- Awareness creatie
  De FRZV wenst te benadrukken dat de nodige awareness voor deze problematiek in de organisaties primordiaal is. Elke medewerker in een ziekenhuis heeft hier een verantwoordelijkheid, zoals ook bij herhaling in de evaluatie van incidenten blijkt. Ondanks het feit dat in heel wat ziekenhuizen terecht de focus op de technische implementatie van oplossingen wordt gelegd, is het handhaven van een beleid dat de betrokkenheid van de medewerkers een hoeksteen voor een succesvol beleid. In het eerste advies werd door de FRZV gepleit voor de formule van e-learning om medewerkers vertrouwd te maken met richtlijnen en veiligheidsmaatregelen.
  Zie Aanbeveling: Een toereikende structurele financiering voorzien

- Meting van de maturiteit van de organisatie en het in kaart brengen van de risico's
  Een andere belangrijke stap is het bepalen van de maturiteit en het in kaart brengen van de belangrijkste risico's en prioriteiten ter remediëring. Het is daarbij van belang dat het ziekenhuis zich kan positioneren ten opzichte van een minimale norm (zie ook verder).

Zie Aanbeveling: Een referentie – framework voor cyber security uitwerken

- Opstellen van een volwaardig (nood)plan gericht op cybersecurity
  Bovenstaande risico-analyse en maturiteitsmeting kan als basis dienen voor het opstellen van een (nood)plan in geval van een incident (Incident Response Plan), als onderdeel van het globale noodplan voor het ziekenhuis voor zover nog niet aanwezig. De recente cyberincidenten hebben aangetoond dat de nood om terug te vallen op protocollen en richtlijnen erg groot is.
  Zie Aanbeveling: Incident Response plan: templates uitwerken en ervaringsuitwisseling organiseren

- Samenbrengen van expertise en beschikbaar stellen van deze expertise
  De FRZV stelt vast dat het niet evident is om de specifieke expertise voor cybersecurity in de context van de ziekenhuiszorg op te bouwen en te onderhouden. Ziekenhuizen zijn onvoldoende in staat gespecialiseerde profielen aan te trekken. Daarenboven combineren ICT medewerkers van ziekenhuizen typisch meerdere taken. Doet men een beroep op externe expertise, dan is kennis van de specificiteit van een ziekenhuis vaak een probleem. Om die redenen is het poolen van, zowel interne als externe, expertise een interessante piste die verdere uitwerking verdient.
  Zie Aanbeveling: Creëren van een emergency response team ("Z-Cert")

- Ervaringsuitwisseling tussen ziekenhuizen
  In omstandigheden waarin het niet evident is om voldoende expertise op te bouwen (zie hierboven) is het uitwisselen van ervaringen en inzichten een manier om fouten te vermijden, leercurves te verkorten, … om efficiënter de beperkte middelen in te zetten. Een groot aantal ziekenhuizen organiseert dergelijke uitwisseling reeds onderling. Vraag is hoe de bestaande inzichten van binnen en buiten onze ziekenhuizen zo goed mogelijk samengebracht en gedeeld kunnen worden.
  Zie Aanbeveling: Creëren van een platform voor ervaringsuitwisseling tussen de ziekenhuizen

- SIEM/SOC
  Zoals ook reeds vermeld in het vorige advies wordt de installatie van een SIEM ("Security Information and Event Management") of een SOC ("Security Operations Center") als essentieel beschouwd. Constante 24 op 7 monitoring van eventuele bedreigingen laat toe om cyberattacks te anticiperen. De FRZV stelt vast dat de sector dit als prioriteit aanziet binnen een efficiënt en afdoend cybersecurity beleid.
  Zie Aanbeveling: Uitwerken van een SOC/SIEM voor de Belgische ziekenhuizen

- Technische ingrepen
  Tot slot mag niet over het hoofd worden gezien dat het vooral technische/technologische ingrepen binnen het individueel ziekenhuis zijn die het risico op een cyber aanval verlagen: software licentiëren en hardware installeren die ingrijpt op de bestaande processen en architectuur. Vele ziekenhuizen weten wat zij moeten doen om een bepaalde risico's in te dekken, maar beschikken hiervoor simpelweg niet over de nodige middelen.
  Zie Aanbeveling: Een toereikende en structurele financiering voorzien

4. *Specifieke problematiek*

Zoals al aangegeven in het vorig advies zijn er nog enkele bijkomende problemen die de FRZV wenst aan te kaarten.

- Verzekerbaarheid van het risico op cyberattack
  De FRZV stelt vast dat de verzekerbaarheid van het risico op cyberattack vanuit de verzekeringssector wordt afgewezen. Het gaat niet langer alleen om verhoging van premies, maar eenvoudig het niet in de verzekeringsportefeuille willen opnemen van dit risico. Vanzelfsprekend heeft dit voor de sector belangrijke gevolgen. Het is voor de FRZV een evolutie die onaanvaardbaar is.

- Financiering van gerelateerde functies in het ziekenhuis
  In het vorig advies werd ook al verwezen naar de verplichting van de ziekenhuizen om sinds enkele jaren een informatieveiligheidsadviseur en een DPO in dienst te nemen zonder dat hiervoor een financiering voorzien is. Binnen de context van de problematiek van de cybersecurity kan de rol van deze functies in een ziekenhuis niet onderschat worden. Zij spelen een cruciale rol in het ganse traject van cybersecurity. De FRZV doet dan ook andermaal een oproep tot de minister om een gepaste financiering te voorzien voor deze functies in het ziekenhuis.

- Regelgeving
  In Nederland wordt het verbod om losgeld te betalen in geval van hacking bekeken. Dit zou de incentive voor hackers grotendeels wegnemen. Er kan onderzocht worden of soortgelijke wetgeving ook in België nuttig kan zijn. Een tegenargument hiervoor is dat hackers zich dan wellicht zullengaan toeleggen op de organisaties die het meest kwetsbaar zijn omwille van een specifieke problematiek, bv. ziekenhuizen.
  Zie ook in de US: Ransomware and Financial Stability Act

5. *Concrete aanbevelingen voor de overheid*

- **Een toereikende en structurele financiering voorzien**
  Voor meer details: zie financieringsmechanisme

- **Ondersteunen van awareness creatie rond cyber security binnen de ziekenhuizen**
  Dit kan gebeuren door deze acties in aanmerking te nemen voor financiering. Zie ook: financieringsmechanisme.

- **Een referentie – framework voor cyber security uitwerken**
  We beschikken vandaag over een set van minimale normen (https://www.ehealth.fgov.be/ehealthplatform/nl/minimale-normen-ziekenhuizen) die het startpunt kan vormen van de uitwerking van een framework dat geschikt is als technische instrument voor:
  - Inschatting van individuele maturiteit en risico's van een ziekenhuis
  - Benchmarking tussen ziekenhuizen
  - Gestructureerde ervaringsuitwisseling

  De FRZV stelt voor om een werkgroep op te richten die een dergelijk framework kan samenstellen en onderhouden. Deze werkgroep zou met andere woorden een permanent karakter hebben.

- **Creëren van een platform voor ervaringsuitwisseling tussen de ziekenhuizen**
  Dit platform moet toelaten informatie over het geheel van de ziekenhuizen zo goed mogelijk uit te wisselen. Deze aanbeveling wordt reeds in de praktijk gebracht.

- **Incident Response plan: templates uitwerken en ervaringsuitwisseling organiseren**
  Aan de hand van templates en via onderlinge uitwisseling kunnen ziekenhuizen hun plannen opstellen of bijsturen. Deze aanbeveling wordt reeds in de praktijk gebracht via een werkgroep die zich hierover buigt.

- **Uitwerken van een SOC/SIEM voor de Belgische ziekenhuizen**
  Idealiter wordt dit op sectorniveau georganiseerd om aldus middelen en competenties (zelfs externe competentie is schaars) maximaal te poolen. Echter, er is een verregaande afstemming over de ziekenhuizen nodig alvorens een dergelijke SOC collectief kan worden georganiseerd. Zo zal bijvoorbeeld het basis maturiteitsniveau van de deelnemende ziekenhuizen moeten worden afgestemd. Zo niet wordt het organiseren van een collectieve SOC te complex. Daarnaast zal er ook werk moeten gemaakt worden van policies: bv het bepalen van de definitie van een incident, het bepalen van de respons op incidenten, etc.

- **Creëren van een emergency response team ("Z-Cert")**
  De interventieteams die doorgaans ingeschakeld worden in geval van een incident vanuit bv. de verzekeraar of vanuit de overheid, zijn niet altijd vertrouwd met de specificiteit van de ziekenhuissector. Om die reden stelt de FRZV voor om te werken met een sectorspecifiek "Emergency Response Team" dat in deze omstandigheden kan ingeschakeld worden. Het betreft hier medewerkers uit de ziekenhuissector, vertrouwd met de implicaties van een aanval en tevens vertrouwd met de operationele aspecten van een ziekenhuis om de getroffen instelling te ondersteunen. Op die manier kan ook binnen elke organisatie de opbouw van specifieke kennis verzekerd worden. Uitwisselen van kennis en informatie tussen instellingen is ook een belangrijk onderwerp. Deze Z-CERT (Computer Emergency Response Team voor de Zorg) kan nauw samenwerken met het bestaande CERT.be, maar ook met sectorspecifieke Z-CERT teams uit het buitenland. Deze organisatie kan ook de basis vormen voor de pooling van bredere competentie.

- **Het risico van onverzekerbaarheid wegnemen**
  De overheid kan maatregelen nemen om de verzekeringssector aan te zetten hiervoor een oplossing te vinden. De overheid zou ook kunnen overwegen zelf de verzekering van de ziekenhuizen op zich te nemen. Zeker wanneer door de sector stappen worden gezet om de risico's zo goed mogelijk te beheren, is het ongehoord dat wanneer er zich toch incidenten zouden voordoen, de ziekenhuizen hier zelf de financiële gevolgen voor het volle pond zouden moeten dragen.

- **Regelgevende initiatieven overwegen**
  Verschillende landen hebben wetgevende initiatieven in de steigers staan om cyber criminelen te ontraden door de financiële incentive weg te nemen. Ook in België kunnen dergelijke initiatieven worden genomen. De FRZV beseft evenwel dat dit niet tot de bevoegdheden van de minister van Volksgezondheid behoort.

- **Coördinatie**
  Naast het financieren van de ziekenhuizen adviseert de FRZV te investeren in coördinatie van de te nemen initiatieven die hierboven beschreven werden. Het samenstellen van een framework, het in kaart brengen van het marktaanbod voor SOC services, het zijn maar een paar voorbeelden waarvoor het samenbrengen van werkgroepen niet zal volstaan. Daarom pleit de FRZV voor het uitschrijven van een opdracht voor de inhoudelijke en projectmatige begeleiding van de te nemen initiatieven.

6. <u>Financieringsmechanisme</u>

In het vorig advies werd een inschatting gemaakt over de kosten verbonden aan de verschillende stappen in de uitbouw van cybersecurity in de ziekenhuizen.

De FRZV wil hier nogmaals herhalen, zoals in de inleiding reeds aangegeven, dat een financiële input vanuit de overheid van 20 miljoen euro zeker wordt gewaardeerd. Het feit dat het om een éénmalige investering gaat, staat evenwel haaks op de continuïteit die dient gewaarborgd te worden en het cyclisch karakter van bv. de evaluatie en updating van de graad van bescherming. De FRZV pleit dan ook voor een structurele, recurrente financiering om de cybersecurity in de ziekenhuizen te ondersteunen en uit te bouwen.

- <u>A priori verdeling AZ-PZ</u>

  De FRZV stelt voor deze verdeling, analoog aan de BMUC financiering, te bepalen volgens de relatieve verhouding binnen het BFM-budget voor beide sectoren. Dit komt overeen met een 85,5% (AZ) -14,5% (PZ) verdeling. Deze voorafgaande verdeling van de beschikbare middelen laat toe om specifiek budget voor beide sectoren te identificeren en te verzekeren. Voor de verdere toewijzingsmechanismes maakt de FRZV op dit moment geen onderscheid tussen AZ en PZ.

- <u>Verdeling over de ziekenhuizen</u>

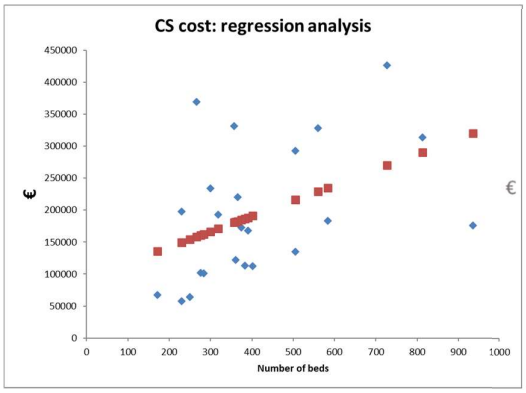
  Vermits men voor cyber security niet over een gepast framework beschikt, is het op de korte termijn niet mogelijk om de financiering te baseren op een systeem analoog aan BMUC, namelijk het financieren op basis van het bereiken van bepaalde stappen. Net zoals bij de EPD-financiering stelt de FRZV wel voor om in de toewijzing van de financiering aan elk ziekenhuis een vaste (vast bedrag per ziekenhuis) en een variabele (in functie van het aantal bedden) component te voorzien die het ziekenhuis kan inzetten voor een aantal vooraf bepaalde ingrepen volgens het eigen maturiteitsniveau. Op die manier kan men de eerstvolgende noden binnen het ziekenhuis afdekken en een efficiënte(re) inzet van de middelen garanderen. De overheid dient hiervoor, idealiter in samenwerking met de ziekenhuizen) een overzicht aan te leggen van de acties/ingrepen die in aanmerking komen. Een aantal hiervan kwamen reeds aan bod:

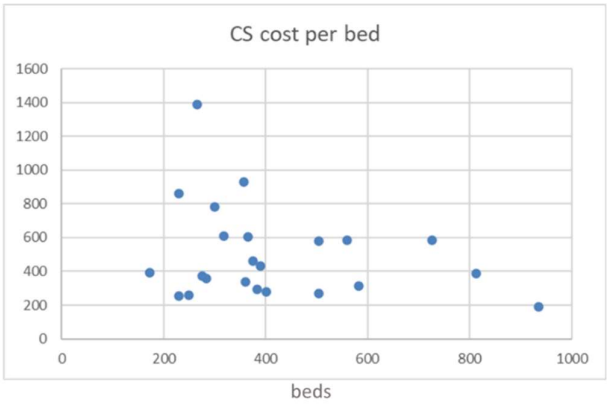
  - Awareness creatie
  - Risico-inventarisatie
  - Incident response planning
  - SIEM/SOC
  - Technische/technologische ingrepen

Wat deze laatste betreft is het in sommige gevallen niet makkelijk om onderscheid te maken tussen ingrepen die verondersteld onderdeel uit te maken van de uitbouw van de ziekenhuis-infrastructuur en ingrepen die specifiek voor cyber security noodzakelijk zijn (back-up is hiervan een goed voorbeeld). Een goede argumentatie van deze noodzaak is bijgevolg noodzakelijk.

- <u>Vast en variabele component</u>

  Uit de bevraging van Zorgnet-Icuro over de kosten voor cyber security in 2020 komen volgende figuren:





Deze bevestigen in de eerste plaats het grote maturiteitsverschil (verondersteld dat men dit toch enigszins kan afleiden uit de uitgaven).

Het is ook duidelijk dat de kleinere ziekenhuizen proportioneel meer uitgeven. Hieruit concludeert de FRZV dat de vaste component van de financiering vrij aanzienlijk zou moeten zijn, temeer omdat een te klein percentage het bedrag al te zeer zou reduceren voor de kleinere ziekenhuizen om nog betekenisvol te zijn. De FRZV stelt daarom voor om 50% van het budget per sector te verdelen pro rata het aantal ziekenhuizen en 50% op basis van het aantal bedden en plaatsen.

- <u>Financiering op lange termijn</u>

  De FRZV stelt voor de financiering op de langere termijn te baseren op het te ontwikkelen framework naar analogie met BMUC. Op die manier kan maturiteit in rekening worden gebracht en kan er structureel gewerkt worden aan een minimaal maturiteitsniveau voor het geheel van ziekenhuizen.