nazb

netwerk acute zorg brabant

augustus 2024

Ketenoefening cyberaanval

29 & 31 mei: een terugblik

www.nazb.nl

‘Ketenoefening biedt leerlijn voor de toekomst’

We leefden maanden toe naar de Brabantbrede intersectorale ketenoefening cyberaanval. 26 zorgorganisaties namen deel, met betrokkenheid van ruim 450 deelnemers. Tijdens de oefendagen zagen we bij hen veel enthousiasme. Daarvoor spreek ik, ook namens het Dagelijks Bestuur ROAZ, mijn grote dank uit. De wijze waarop jullie zijn omgegaan met de dilemma’s, uitdagingen en onzekerheden waarmee we als acute zorgketen te maken krijgen tijdens een cyberincident, verdient een groot compliment.

Een cyberincident is een realistisch scenario. De technologische en digitale ontwikkelingen in de zorg namen de afgelopen jaren een vlucht. Een recent voorbeeld is de wereldwijde ICT-storing, waarbij miljoenen Windows-computers werden getroffen door foute update van beveiligingsbedrijf CrowdStrike. Diverse ziekenhuizen in Nederland ondervonden hinder van die storing.

Door de coronaperiode weten we dat we elkaar kunnen vinden in tijden van crises. We leverden in Brabant destijds een megaprestatie; de zorgcontinuïteit is altijd geborgd geweest. Er ligt een stevig netwerk om in te zetten. Een cyberaanval kent echter specifieke kenmerken en uitdagingen. Het is daarom van belang om als keten voorbereid te zijn op dit type crisis en inzicht te krijgen in de ketenbrede impact, de communicatielijnen en bijbehorende dilemma’s.

Wat als meerdere zorgorganisaties tegelijkertijd gehackt worden, de zorgcontinuïteit in gedrang komt, en van sommigen ransomware wordt geëist? Welke zaken vragen om regionale planvorming? Dankzij deze ketenoefening ligt er een mooie leerlijn voor de toekomst, die jullie in dit document terugvinden. We kunnen ons nu beter voorbereiden, wat vertrouwen biedt voor de toekomst.

Nogmaals bedankt voor jullie betrokkenheid, toewijding en enthousiaste inzet!

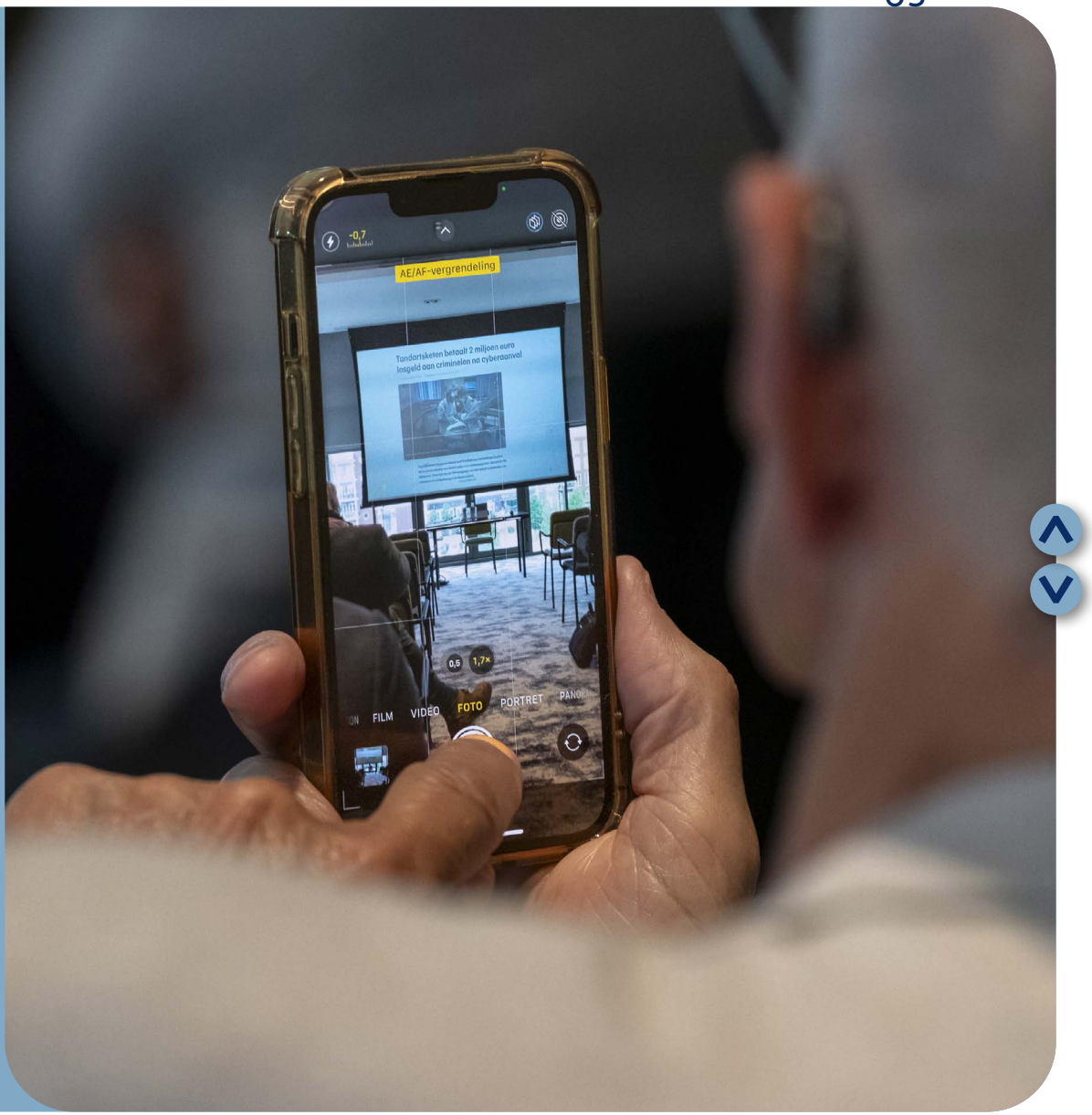
Bart Berden
voorzitter ROAZ Brabant

Over dit document

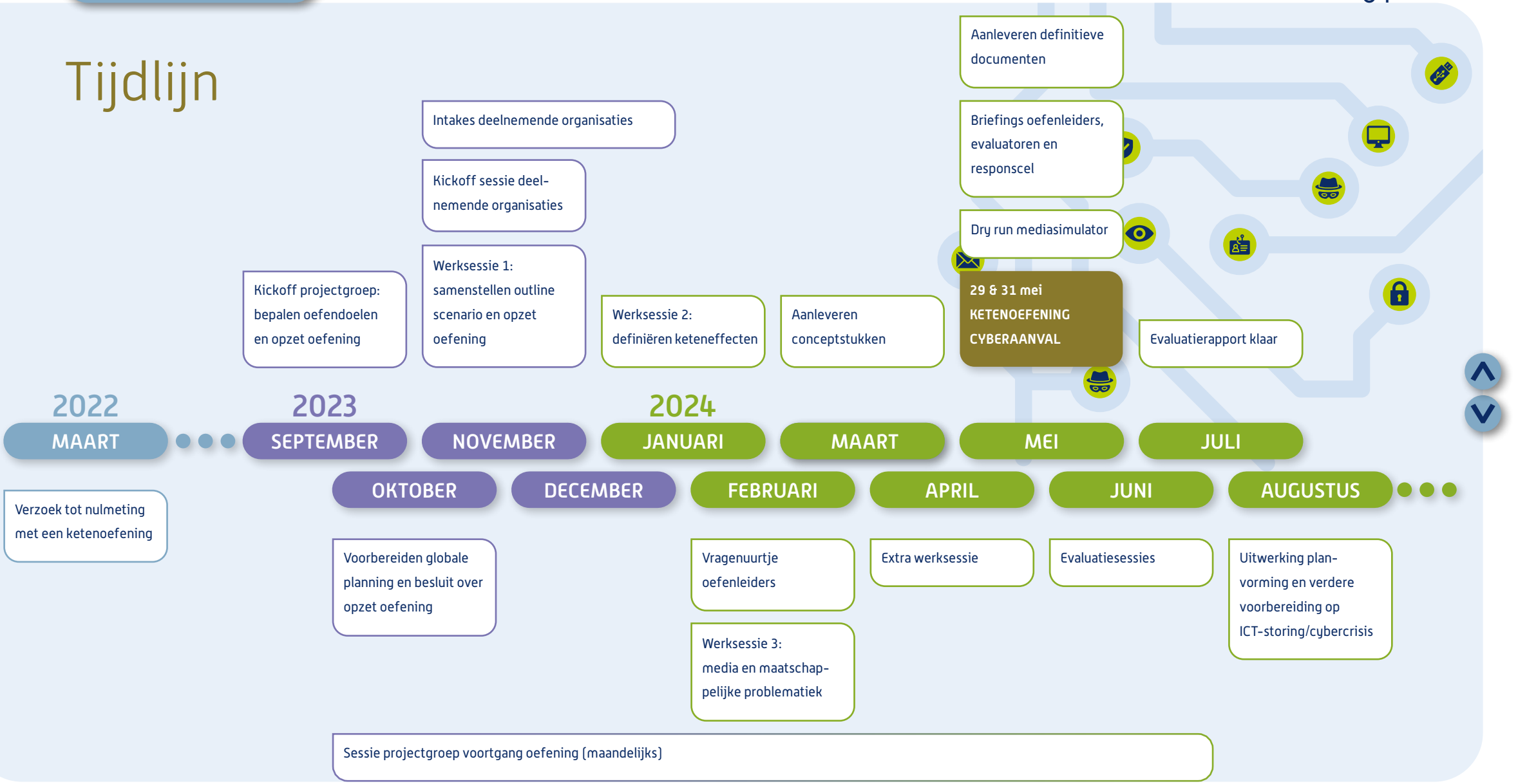
Het COT, die NAZB bij de totstandkoming van deze ketenoefening cyberaanval begeleidde, heeft een evaluatierapport opgesteld. Deze uitgave geeft een terugblik op de oefening en zet de observaties en conclusies op een rij. Deelnemers aan de ketenoefening kunnen het volledige evaluatierapport van het COT opvragen via secretariaat@nazb.nl.

Klik op het kopje om naar het hoofdstuk te gaan

Inhoudsopgave



Tijdlijn


Aanleveren definitieve documenten
Intakes deelnemende organisaties
Briefings oefenleiders, evaluatoren en responscel
Kickoff sessie deel-nemende organisaties
Dry run mediasimulator
Kickoff projectgroep: bepalen oefendoelen en opzet oefening
Werksessie 1: samenstellen outline scenario en opzet oefening
29 & 31 mei KETENOEFENING CYBERAANVAL
Werksessie 2: definiëren keteneffecten
Aanleveren conceptstukken
Evaluatierapport klaar
2022
2023
2024
MAART
SEPTEMBER
NOVEMBER
JANUARI
MAART
MEI
JULI
OKTOBER
DECEMBER
FEBRUARI
APRIL
JUNI
AUGUSTUS
Verzoek tot nulmeting met een ketenoefening
Voorbereiden globale planning en besluit over opzet oefening
Vragenuurtje oefenleiders
Extra werksessie
Evaluatiesessies
Uitwerking plan-vorming en verdere voorbereiding op ICT-storing/cybercrisis
Werksessie 3: media en maatschap-pelijke problematiek
Sessie projectgroep voortgang oefening (maandelijks)

Ketenoefening cyberaanval: hoe kwam het tot stand?

Bijna een jaar lang is NAZB samen met het COT en de ketenpartners bezig geweest met de voorbereiding van de ketenoefening cyberaanval. Wat ging hier allemaal aan vooraf?

Waarom een grote ketenoefening over een ICT-storing/cyberaanval?

Zorgorganisaties zijn wettelijk verplicht om onder alle omstandigheden de bereikbaarheid, toegankelijkheid en kwaliteit van de zorg te borgen. Al jaren neemt de dreiging op ICT-uitval door cybercriminaliteit toe. Landelijk en internationaal zijn er legio voorbeelden waarbij zorgorganisaties getroffen zijn door hackers. De dreiging op ICT-uitval binnen de zorg door cybercriminaliteit vormt een groot risico. Het is belangrijk om daar goed op voorbereid te zijn, als individuele organisatie én als acute zorgketen. Wat is de impact op de zorgcontinuïteit als ROAZ-regio Brabant getroffen wordt? Welke maatregelen en handelingsperspectieven hebben we dan om de bereikbaarheid, toegankelijkheid en opvang van de acute patiënten te borgen? De Brabantse zorgorganisaties bereidden zich de afgelopen jaren voor op wat ze moeten doen als ze te maken krijgen met cybercriminaliteit. Het is echter van belang om ook als keten voorbereid te zijn.

Hoe zijn we de afgelopen jaren als keten met dit onderwerp bezig geweest?

Op 28 juni 2017 vond er een netwerkdag plaats rondom het thema 'Langdurige ICT-uitval en cybersecurity'. Deze themadag was de aftrap voor zorgorganisaties om zich bewust te worden van de steeds grotere afhankelijkheid die zorgprocessen hebben van de digitale middelen en wat dat voor dreigingen en risico's heeft. Met behulp van het OTO-stimuleringsprogramma gingen ketenpartners aan de slag binnen de eigen zorgorganisaties om de bewustwording van de risico's van cybercriminaliteit te vergroten en planvorming op te stellen. Daarnaast werden sleutelfunctionarissen getraind in hun rol, de mogelijke dilemma's en het nemen van kritieke besluiten daarin.

De focus op het programma gericht op de voorbereiding van de individuele zorginstellingen duurde tot 2019. In 2019 gaf het ROAZ opdracht om te kijken naar de keteneffecten en de voorbereiding daarop. In de periode 2020 - 2021 lag het OTO-programma nagenoeg stil vanwege corona. In 2022 is het thema cybercriminaliteit in Brabant opgepakt. Tijdens een expertgroepbijeenkomst ICT en crisisbeheersing lichtte netwerkbureau Euregio toe hoe die het programma rondom digitale ontwrichting in de keten heeft uitgevoerd. Naar aanleiding van die presentatie ontstond de vraag wat er nodig is aan specifieke planvorming voor ketenbrede effecten bij digitale uitval. Daarop is het besluit genomen om een intersectorale ketenoefening te organiseren als een nulmeting om te bepalen wat er aan specifieke planvorming wordt gevraagd rondom cybercriminaliteit.

Wanneer vond de laatste grote ketenoefening plaats?

De laatste keer dat er een grote intersectorale ketenoefening werd gehouden, was in 2019, die in het teken stond van een infectieziekteuitbraak. Dat was een goede voorbereiding op de coronacrisis die volgde. Als regio vinden we het belangrijk dat bepaalde thema's die keteneffecten hebben ketenbreed worden beoefend om voorbereid te zijn op crisissituaties. Zo is tweemaal de infectieuitbraak beoefend (2016 en 2019), oefenden we in 2024 een ICT-storing/cyberaanval en staat een volgende oefening rondom evacuatie van een ziekenhuis in 2026 op de planning.

Een cybercrisis manage je met elkaar

‘Als je een beetje het nieuws volgt, dan weet je dat een cyberaanval de zorg op de hielen zit. En als een zorgorganisatie eenmaal getroffen wordt, kan een cyberaanval zo de gehele bedrijfsvoering platleggen. Zorgorganisaties zijn gewoon heel kwetsbaar. Daarom is het goed dat we dit scenario ketenbreed hebben beoefend. Een cyberaanval vergt echt een andere aanpak dan een ICT-storing. Alleen al vanwege de ethische dilemma’s die erbij komen kijken, zoals het wel of niet betalen van ransomware. Het is heel mooi dat we dat met elkaar hebben mogen oefenen. De oefening diende als een nulmeting. We weten nu hoe we ons nog beter kunnen voorbereiden binnen het ROAZ op een cybercrisis. Tegelijkertijd ben ik blij dat de dingen waar we goed in zijn, juist ook goed verliepen tijdens deze oefening. Alle sectoren wisten elkaar onderling en over de gehele breedte te vinden. Ik heb dezelfde saamhorigheid teruggezien als tijdens de coronacrisis. Daar heb ik van genoten. Die relaties opbouwen en warmhouden is misschien wel het belangrijkste. Het is essentieel om goed voorbereid te zijn en crisis- en opschalingsplannen klaar te hebben liggen, maar een cybercrisis manage je met elkaar.’

Robert Janssen
zorgmanager ETZ en voorzitter Tactisch Kernteam

Tijdens de oefening wisten sectoren elkaar onderling en over de gehele breedte te vinden.

De ketenoefening: opzet, scenario en oefendoelen

Voordat we de observaties en aanbevelingen doornemen, blikken we terug naar 29 en 31 mei. Wat hebben we gedaan tijdens de oefendagen?

Opzet

De oefening bestreek drie dagdelen. Tijdens de eerste twee dagdelen werd interactief geoefend. Het laatste dagdeel werd benut voor een eerste terugkoppeling van de oefening en een **thema-middag.** De oefening werd aangestuurd door de centrale oefenleiding en er waren twee responscellen die het tegenspel verzorgden (algemeen en media/communicatie). De centrale oefenleiding en beide responscellen kwamen fysiek bijeen. Tijdens de oefening was er een strak vergaderschema om recht te doen aan de oefendoelen en om de overleggen van het Tactisch Kernteam en DB ROAZ goed te betrekken in de oefening. Dat liet wat minder ruimte voor spontane acties zoals in reguliere oefeningen. Er vonden vijf (vooraf ingeplande) overleggen plaats: Tactisch Kernteam, sectoraal strategisch ROAZ ziekenhuizen en regionale ambulancevoorzieningen, sectoraal strategisch ROAZ huisartsenzorg, DB ROAZ en bijeenkomst crisiscommunicatie.

Het scenario

Het scenario betrof een cyberaanval met impact op de (acute) zorgketen. Het scenario vulden de deelnemers zelf in tijdens bijeenkomsten met scenariowerkgroepen. Het hoofdscenario was opgebouwd vanuit één of meerdere criminele organisaties die cyberaanvallen uitoefenen op willekeurige organisaties. Via een kwetsbaarheid in de netwerkmonitoringsoftware van PolarBreeze (fictieve leverancier), krijgen hackers toegang tot netwerken van zorgorganisaties. In de loop van de oefening ontstaan problemen in de ICT-omgevingen van organisaties. Er volgen steeds meer reacties vanuit media en politiek. Soms lukt het criminele organisaties om ransomware uit te rollen over de netwerken van zorgorganisaties en losgeld te vragen om systemen te herstellen of te voorkomen dat gevoelige gegevens naar buiten worden gebracht.

Oefendoelen

Tijdens de intersectorale oefening lag de focus op ketensamenwerking, communicatie en borging van de zorgcontinuïteit in ketenverband bij een ICT-storing/cyberaanval binnen ROAZ-regio Brabant. Hoewel technische aspecten van een hack werden meegenomen, lag de nadruk op leren en niet op testen. De oefening diende als nulmeting om te evalueren of de mensen, betrokken bij de bestrijding van een cybercrisis, elkaar weten te vinden, de geldende afspraken kennen en deze met elkaar kunnen toepassen en te identificeren waar aanpassingen nodig zijn. De oefening biedt daarom nieuwe inzichten voor effectieve crisisbestrijding in de toekomst. Doelstellingen voor deze oefening zijn:

OEFENDOEL 1

Inzicht verkrijgen in:

- de (ketenbrede) impact (of gevolgen) van cyber/digitale ontwrichting op zowel de interne- als regionale (acute) zorgcontinuïteit:
- behoeften van de ketenpartners in de voorbereiding op een cybercrisis;
- informatie- en communicatielijnen tussen partijen tijdens een cyberincident.

OEFENDOEL 2

Awareness creëren en risicobewustzijn vergroten rondom het scenario cyber/digitale ontwrichting.

OEFENDOEL 3

Leerpunten ontdekken die niet eerder naar boven zijn gekomen (blind spots) en die vragen om regionale planvorming.

De maatschappelijke en politieke beeldvorming vragen om een eenduidige samenwerking en woordvoering door de hele keten. Er is niet daadwerkelijk geoefend met de technisch/operationele onderdelen van het scenario. Het scenario en de impact verschilde per organisatie.
Tijdens de oefening op 29 en 31 mei stond de interactie tussen de betrokken partijen en de coördinatie centraal. Het hoofdscenario kende drie hoofdlijnen: de technische lijn met daarin de cyberontwikkelingen en dreiging op uitval in de zorgregio, de impact op de zorgketen en de maatschappelijke dynamiek en ontwrichting vanuit de beeldvorming, mediadynamiek en maatschappelijk sentiment. Voor een goede respons en het maximaal beperken van de impact op de (acute) zorgketen, was onderlinge afstemming en coördinatie nodig.

Oefenbeperkingen en oefenwinst

Een oefening is altijd een vereenvoudiging van de werkelijkheid en kent daardoor beperkingen op het verloop en daarmee op de leerpunten. Dat geldt ook voor deze ketenoefening. Een voorbeeld is dat organisaties tijdens een oefening niet alle capaciteit kunnen inzetten die zij in werkelijkheid wel zouden vrijmaken. De normale werkzaamheden gaan immers door. In een oefening ervaren deelnemers niet de werkelijke druk en krijgen ze niet de zeer grote hoeveelheid reacties, telefoontjes, appjes en dergelijke. Een laatste beperking is dat in de oefening sommige teams alleen de geplande overleggen hadden en weinig tijd tussen die overleggen.
Naast deze beperkingen zijn er voordelen bij een oefening die het crisismanagement bevorderen en die in een werkelijke situatie anders zullen lopen. Zo is de oefening voorbereid, de betrokken functionarissen weten wanneer deze plaatsvindt en ‘staan klaar’ om direct in actie te komen.
In werkelijkheid kost het opstarten meer tijd. Daarnaast is tijdens de oefening een deelnemerslijst beschikbaar met contactgegevens, wat in de praktijk vaak ontbreekt. Een voordeel van de meer geregisseerde aanpak waarvoor in deze oefening gekozen is, is dat de deelnemers hebben ervaren hoe het kan zijn als het goed geregeld is.

De responscellen algemeen en media verzorgden het tegenspel tijdens de ketenoefening.

Niet de vraag óf, maar wanneer we getroffen worden

'De ketenoefening cyberaanval was voor mij behoorlijk intensief, omdat ik meerdere functies bekleedde: oefenleider, lid van het projectteam en lid Tactisch Kernteam. Die meerdere petten dragen, maakte het uitdagend. Het leert ons ook dat bij een echte crisis er problemen kunnen ontstaan, omdat het onmogelijk is om alles tegelijkertijd te doen. Direct na de ketenoefening vond er in ons ziekenhuis een interne evacuatieoefening plaats. Wat gebeurt er als de volledige bedrijfsvoering stil ligt? Welke vraagstukken komen dan naar boven? Hoe ziet een evacuatieplan eruit? En hoe bouw je, zodra alles weer functioneert, de zorgorganisatie weer op? We hebben een hele hoop goed ingeregeld, maar we kunnen zeker nog slagen maken. Het is niet de vraag óf, maar wanneer de acute zorgketen getroffen wordt. Dat kan sneller gebeuren dan we zouden willen. Denk terug aan de wereldwijde computerstoring van eind juli; die had net zo goed onze zorgorganisatie en regio kunnen treffen. Het maatschappelijke taboe om de gezondheidssector buiten schot te houden, bestaat niet meer. Het was daarom fantastisch om de ketenoefening cyberaanval met meer dan vierhonderd mensen voor te bereiden en daardoor nog meer collega's te leren kennen. De **themamiddag** was daarvoor ook uitstekend. Tot slot wil ik mijn complimenten uitspreken richting Patricia en haar team. Hun prestatie was fantastisch, gezien de hoeveelheid tijd die erin is gestoken. Chapeau!'

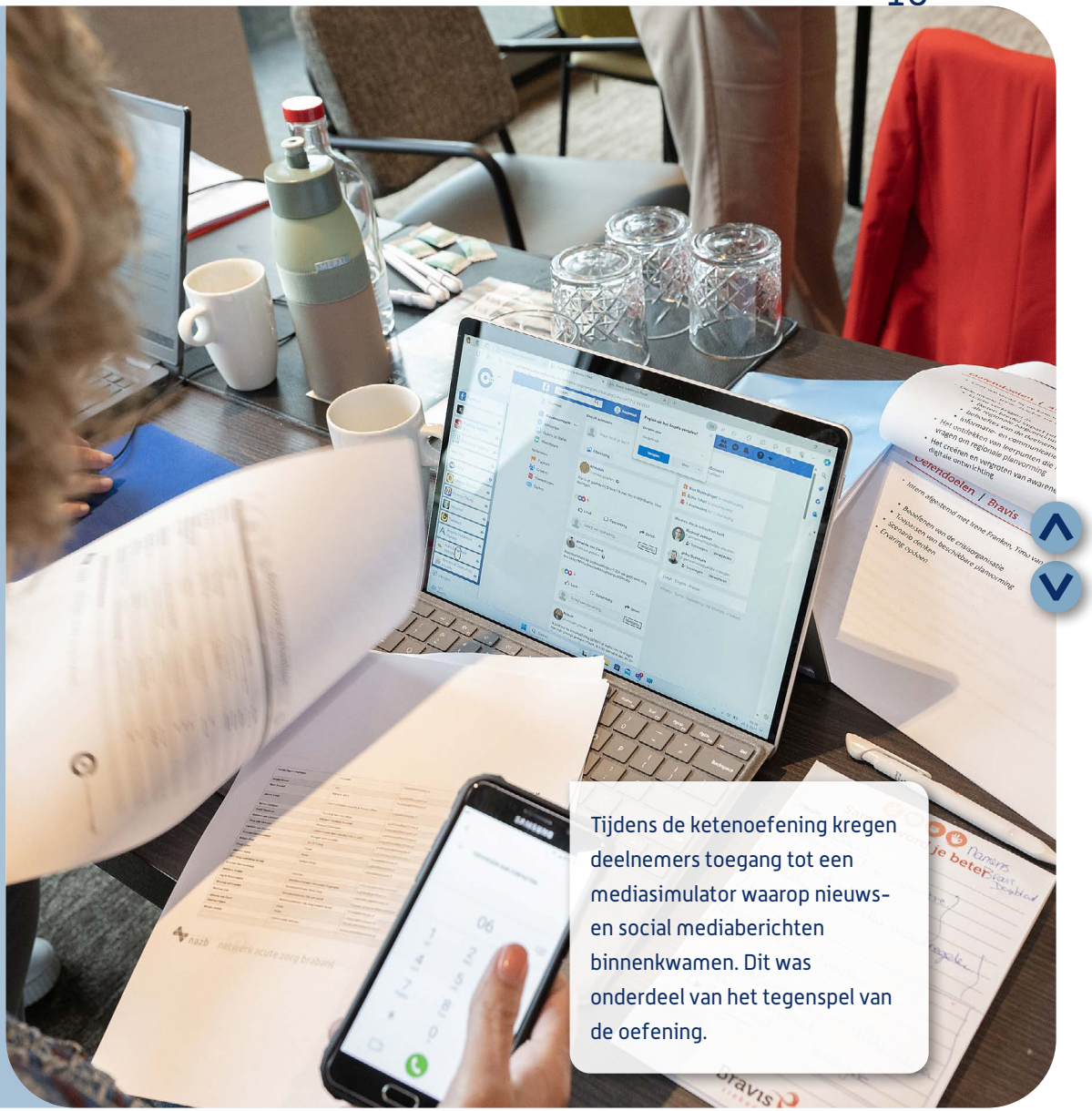
Lotte Rijksen
manager zorg en bedrijfsvoering JBZ

De ketenoefening cyberaanval kwam tot stand mede door de betrokkenheid van ruim 450 deelnemers.

Cyber een reëel thema om te oefenen

'Ik kijk met een goed gevoel terug op de intersectorale ketenoefening. Super dat we dit keten- en regiobreed hebben geoefend. In april begon ik bij GHOR Brabant Midden-West-Noord. Ik ben in mijn rol als oefenleider dus gelijk in het diepe gesprongen. Erg leuk om te doen, omdat het zo'n belangrijk thema is: de kans is groot dat je als organisatie getroffen wordt door cybercriminaliteit. Een dergelijke aanval heeft een enorme impact op de samenleving en dus ook op de zorg. Dat bleek wel tijdens de twee oefendagen.
De samenwerking verliep naar wens. Mooi om te zien dat, ondanks er in het oefenscenario geen GRIP-opschaling was, de geneeskundige partners de GHOR weten te vinden en dat we het nut en de noodzaak van netcentrisch samenwerken opnieuw hebben kunnen laten zien. Het is prettig dat we laagdrempelig met de keten in verbinding hebben gestaan. Het geeft ons allemaal veel inzichten die aansluiten bij de aanbevelingen van ons onlangs vastgestelde Regionale Zorgrisicoprofiel Brabant Midden-West-Noord. We wisten mooie leerpunten uit de oefening te halen, zoals inventariseren op welke wijze we de ketenpartners kunnen meenemen in een verdieping rondom de netcentrische werkwijze en gebruik van LCMS-GZ. Informatie delen en duiden is tijdens de opgeschaalde zorg immers super belangrijk.'

Erik Verhaagh
beleidsadviseur GHOR Brabant Midden-West-Noord



Tijdens de ketenoefening kregen deelnemers toegang tot een mediasimulator waarop nieuws- en social mediaberichten binnenkwamen. Dit was onderdeel van het tegenspel van de oefening.

Observaties uit het evaluatierapport

Het COT heeft de belangrijkste observaties van de ketenoefening cyberaanval in zeven thema's samengevat in een evaluatierapportage. Deelnemers aan de ketenoefening kunnen het volledige evaluatierapport van het COT opvragen bij het secretariaat van NAZB.

Geslaagde oefening; positieve feedback van deelnemers

De oefening is gemiddeld beoordeeld met een 8. Deelnemers ervaarden het scenario als realistisch. De opzet met de verschillende scenariolijnen zorgde voor voldoende maatwerk. Voor de voorbereiding was veel waardering. Deelnemers geven wel aan dat ze liever op één dag langer oefenen dan op twee losse dagdelen met een 'freeze' ertussen.

Awareness is groot en gegroeid

PAST BIJ OEFENDOEL 3 >>

90% van de deelnemers zegt dat de awareness rondom cybercriminaliteit is gegroeid. De voorbereiding van de oefening hielp daarbij, hoewel sommigen aangaven dat de voorbereiding korter en eenvoudiger kon. Er is meer inzicht ontstaan in zowel de impact binnen de eigen organisatie als op de zorgketen. Voor een aantal organisaties is het een bevestiging van de al genomen maatregelen en voor een aantal is de oefening een wake-up call. Vrijwel iedere deelnemende organisatie benoemt een aantal vervolgstappen om de weerbaarheid te vergroten, zoals plannen, maatregelen ten aanzien van zorgcontinuïteit en inzicht in de impact van een ICT-storing/cyberaanval. Daarnaast zeggen de deelnemers inzichten te hebben gekregen in de onderlinge afhankelijkheid, keteneffecten en behoefte te hebben aan regie op de keten.

Regionale afstemmingsmomenten bieden een basis voor een regionale aanpak

PAST BIJ OEFENDOEL 1 >>

De coronaperiode droeg volgens de deelnemers bij aan een stevig regionaal netwerk. Dat vergemakkelijkte de afstemming. De regionale (keten)overleggen worden positief geëvalueerd. Deelnemers zeggen dat het goed is dat er een afstemmingscyclus bestond en de overleggen gedegen voorbereid waren. De voorzitters kregen complimenten over hun vermogen om een goede samenvatting te maken. De overleggen waren belangrijk voor de totstandkoming van een gezamenlijk beeld en gezamenlijke acties en besluiten. Zo zijn afspraken gemaakt over gezamenlijke communicatie en coördinatie op patiëntenspreiding, is gesproken over een prioritering in het herstel van zorgorganisaties en is afgesproken dat gezamenlijk opgetrokken wordt in geval van ransomware. Tegelijkertijd zeggen de deelnemers dat het nog beter kan. Een standaard agenda, actueler en completer situationeel beeld, meer ruimte voor duiding en betekenisgeving op het gebied van cybercriminaliteit en met een duidelijker doel en resultaat voor ieder overleg.
De ondersteunende rol wordt nu op een positieve manier ingevuld door NAZB. Echter, de vraag is of dat bij een intensieve, hoogdynamische en mogelijk langdurige crisis houdbaar is. In de 'warme fase' bestaan momenteel geen formeel ondersteunende rollen vanuit NAZB, zoals een ICO of plotter. Een andere bevinding betrof de aansluiting van de GHOR op tactisch niveau en welke rol die vervult daarin, in het bijzonder met het oog op het delen en ophalen van informatie.

Regionale leiding en coördinatie is nog onduidelijk

PAST BIJ OEFENDOEL 1 EN 2 >>

Alle deelnemers vinden samenwerking nodig tijdens een cybercrisis. Ook zien ze dat regie nodig is voor gezamenlijke beeld- en besluitvorming die de hele keten aangaat, bijvoorbeeld patiënten-

spreiding en de verdeling van schaarste in (cyber)capaciteit. Tijdens de oefening verliep dat redelijk goed conform de vastgelegde ROAZ-structuur. Toch is deze structuur niet voor iedereen duidelijk. De rolverdeling tussen GHOR en ROAZ is tijdens de oefening niet altijd helder als het gaat over patiëntenspreiding. Het doel en de functie van de sectorale overleggen zijn niet voor iedereen helder gecommuniceerd waardoor de input en efficiency van die overleggen nog niet op orde zijn. Tijdens de oefening benoemen de voorzitters het doel niet expliciet; de verwachtingen en de input per deelnemer kunnen verschillen. Daarnaast is het niet voor iedereen helder wie verantwoordelijk is voor op- en afschalen en voor het organiseren van het afstemmingsproces. NAZB ondersteunde en organiseerde het afstemmingsproces en zorgde voor de voorbereiding en structuur. COT stelt de vraag of NAZB dit te allen tijde kan leveren. Verder is nog niet geregeld hoe de afstemming met Z-Cert en eventuele coördinatie op de samenwerking tussen ICT-specialisten verloopt.

Belang van informatie-uitwisseling wordt erkend én mag nog beter

PAST BIJ OEFENDOEL 1 >>

De sectorale overleggen droegen bij aan een gezamenlijk beeld. Daarnaast is informatie uitgewisseld in Whatsapp-groepen. Op verschillende plekken werd een mediabeeld bijgehouden en vrijwel alle deelnemers gebruikten LCMS. Daar waren deelnemers blij mee, maar de gezamenlijke beeldvorming/informatie-uitwisseling kan actueler, completer en sneller. Een groot deel van de overlegtijd werd besteed aan de beeldvorming. In alle teams zorgde de voorzitter voor een uitgebreide beeldvormingsronde waarbij alle leden konden aanvullen. Soms ging dat heel beknopt, soms werden details gedeeld die op regionaal niveau weinig toegevoegde waarde hadden. Er was geen informatiecoördinator die het beeld vooraf verzameld had. De beeldvorming ging in op informatie over het cyberincident (technische aard) en de impact op de (acute) zorgcontinuïteit. Die beeldvorming klopte niet altijd met de actuele oefensituatie. In overleg werd soms aangegeven dat er sprake was van beperkte impact bij een organisatie, terwijl in werkelijkheid zorgprocessen waren stilgelegd. De beeldvorming nam veel tijd in beslag waardoor er voor de oordeelsvorming en vooruitdenken beperkt tijd overbleef. Daarnaast benoemden diverse deelnemers dat het gebruik van diverse communicatiemiddelen (whatsapp, LCMS, mail etc.) dubbelop of onduidelijk was.

Gezamenlijke communicatie is van groot belang, én een uitdaging

PAST BIJ OEFENDOEL 1 EN 2 >>

Het overgrote deel van de organisaties communiceerden extern over het incident. De snelheid waarmee gecommuniceerd werd wisselde. Getroffen organisaties zouden snel een eerste bericht kunnen plaatsen, maar niet iedereen deed dat. De organisaties die extern hebben gecommuniceerd, plaatsten berichten op de websites, intranetten en sociale mediakanalen. Een deel verwees naar de website van NAZB. Het communicatiedoel daarbij was informatievoorziening en betekenisgeving. Het principe "praat waar je over gaat" is bij de communicatieprofessionals goed bekend. Vanuit het ROAZ komt de centrale, overkoepelende communicatie en de zorgorganisaties communiceren over hun eigen situatie. Een ruime meerderheid geeft aan de communicatie afgestemd te hebben met andere zorgorganisaties in de regio. De whatsappgroep voor communicatieprofessionals en het ingelaste crisiscommunicatieoverleg gaven daarvoor de belangrijkste input.
De deelnemers zijn voorzichtig positief over de onderlinge afstemming. De centrale regie op het maken van een gezamenlijk omgevingsbeeld ontbreekt, waardoor de beeldvorming veel tijd in beslag neemt. Het crisiscommunicatieoverleg vond plaats wanneer al individueel gecommuniceerd was. Op dat moment wordt het cyberincident al op een verschillende manier geduid: de een spreekt over een cyberaanval en de ander over verstoringen. Tijdens de oefening viel het op dat in de communicatiegroep soms andere beelden bestonden dan in bijvoorbeeld het tactisch overleg.
Bij een cyberaanval is het de uitdaging om te communiceren wat op dat moment bekend is, zonder

onderzoek of opsporing in de weg te zitten of zonder een duiding te geven die formeel nog niet bevestigd is. Deze principes lijken niet bij iedereen bekend. De rolverdeling met cyberspecifieke crisispartijen in relatie tot wie mag communiceren is onduidelijk, denk aan Z-Cert, het National Cyber Security Centrum (NCSC) en de politie.

Regionale planvorming ICT-storing/cyberaanval volgende stap

PAST BIJ OEFENDOEL 2 >>

De oefening is een nulmeting met als doel om regionale planvorming op te stellen. Vooraf was bekend dat er geen regionale plannen voor cybercrises zijn. Meer dan de helft van de deelnemers maakte gebruik van de bestaande, reguliere (regionale) plannen en/of afspraken. In de evaluatie-sessies blijkt dat veel deelnemers niet op de hoogte zijn van deze (regionale) plannen. Voor het grootste deel van de deelnemers is de verwachting vanuit de regio helder als het gaat om informatie-uitwisseling en besluitvorming over een ICT-storing/cyberaanval. Dat was voornamelijk te danken aan ervaringen uit de coronaperiode en aan de uitvraag ter voorbereiding op de sectorale overleggen. Ter conclusie werd bij dit thema gevraagd wat de leerpunten/blinde vlekken zijn die vragen om regionale planvorming:

- informatie-uitwisseling en communicatie;
- mandaten en rolverdeling ten aanzien van leiding en coördinatie regionale acute zorg;
- rolverdeling ROAZ en GHOR;
- regionale afstemmingsproces (vergadercyclus).

De ketenoefening diende als nulmeting met als doel om regionale planvorming op te stellen.

Zwaarste scenario bracht nodige uitdagingen met zich mee

‘Als oefenleider en deelnemer aan de responscel algemeen heb ik de ketenoefening van dichtbij mogen meemaken. Er was veel enthousiasme bij onze medewerkers, want iedereen onderkent het belang van het oefenen van een actueel onderwerp als deze. Met het zwaarste scenario - ons volledige patiëntendossier lag eruit - waren wij als kleine huisartsenspoedpost (HASP) flink getroffen. Zo werden we op de eerste dag al geconfronteerd met een behoorlijke uitdaging. Binnen onze HASP is de ICT uitbesteed bij een extern bedrijf, waardoor die afdeling geen rol had in onze oefening. Als ketenpartner binnen het ROAZ konden wij wel een beroep doen op een forensisch ICT-bedrijf, maar wij stonden als kleine HASP niet bovenaan de prioritering. Daar wil je in de toekomst natuurlijk niet van afhankelijk zijn. De komende tijd gaan we met ons externe ICT-bedrijf aan de slag om het scenario cybercriminaliteit nog beter voor te bereiden. Verder is communicatie een leerpunt. Wij hebben als kleine HASP geen communicatieafdeling, maar mogelijk zouden we kunnen gebruikmaken van de expertise van de communicatieafdeling van het ziekenhuis. Het leukste aan de oefening vond ik dat het een enorm saamhorigheidsgevoel teweegbracht. Ik heb zoveel nieuwe mensen leren kennen, en meer geleerd over de acute zorgketen in Brabant.’

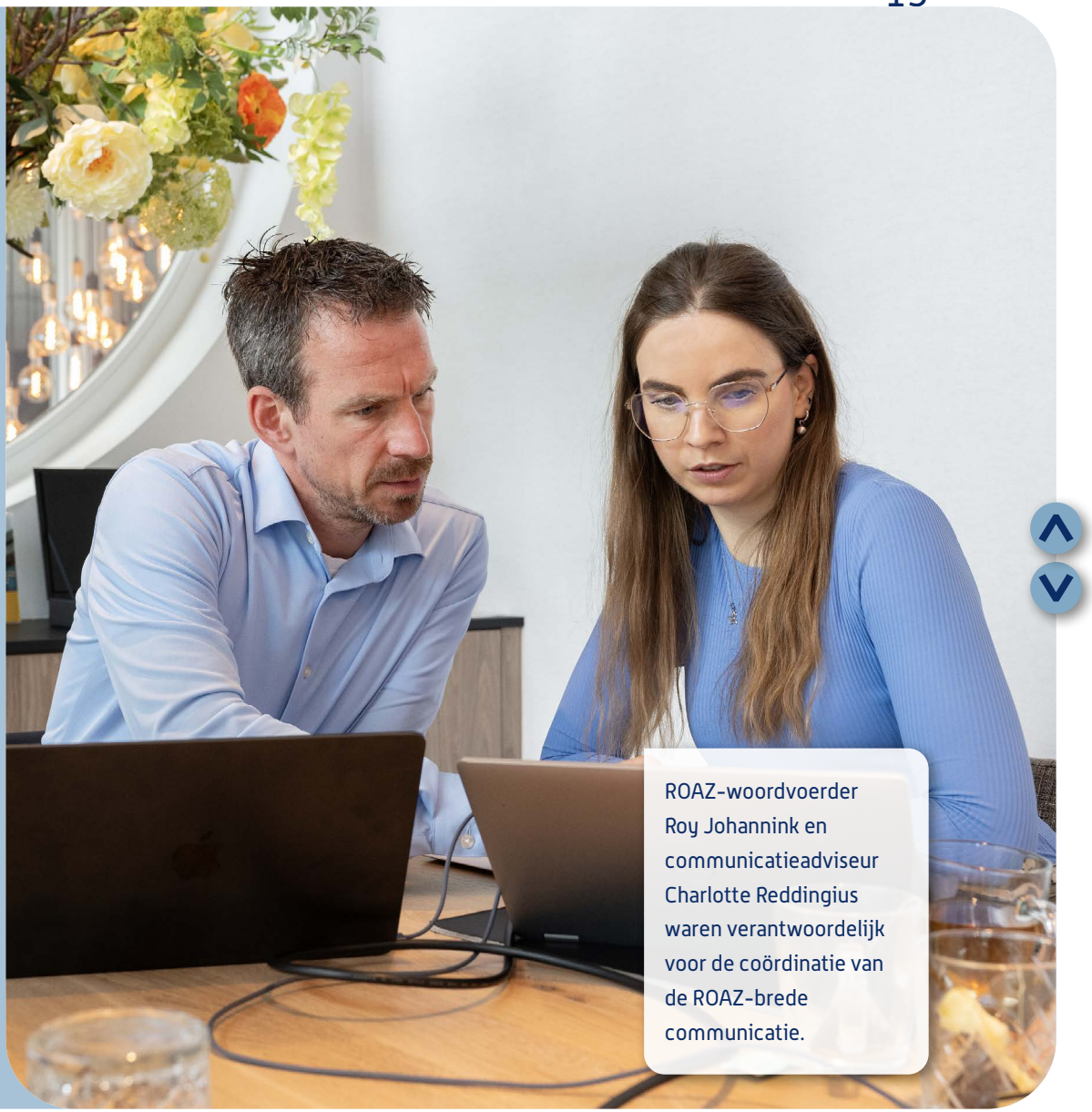
Inge Buss
bestuurssecretaris SHoKo Huisartsenspoedpost

Als oefenleider en deelnemer aan de responscel algemeen maakte Inge Buss de ketenoefening van dichtbij mee.

We kunnen elkaar om hulp vragen

'Tijdens de ketenoefening was ik woordvoerder ROAZ. Samen met Charlotte, communicatieadviseur ROAZ, waren wij verantwoordelijk voor de coördinatie van de ROAZ-brede communicatie en zaten wij de crisisoverleggen met de Brabantse communicatieprofessionals voor. Voorafgaand aan de oefening stelden we planvorming op die we 'in de praktijk' konden toetsen. Het is immers belangrijk om duidelijke afspraken te maken over wie wat communiceert, zodat we weten wat we van elkaar kunnen verwachten. Het eerste kwartier na de start van de oefening werden we als ROAZ al gebeld. De communicatieprofessionals weten ons dus goed te vinden, maar hoe verlopen de communicatielijnen vervolgens? Communiceren we allemaal volgens dezelfde boodschap? Hoe vindt terugkoppeling plaats binnen de interne crisisorganisatie? Het ROAZ heeft een belangrijke rol in de overstijgende communicatie. Maar het is ook essentieel dat iedere organisatie zelfstandig en adequaat communiceert over de eigen specifieke situatie, in afstemming met de andere organisaties. Dat biedt duidelijkheid en voorkomt misverstanden. Een bericht waarin gesproken wordt over een cyberhack wordt heel anders gelezen dan wanneer je praat over ICT-uitval. Tijdens de ketenoefening zaten Charlotte en ik soms aan onze grenzen qua capaciteit. Tegelijkertijd keken communicatieprofessionals naar ons met de vraag voor meer handjes. Gelukkig zijn we met velen en hebben we gezien dat we om hulp kunnen vragen aan collega's. Dat maakt dat we altijd voldoende mankracht hebben om effectief te communiceren.'

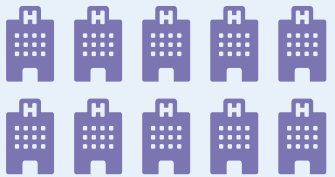
Roy Johannink
trainer crisiscommunicatie



ROAZ-woordvoerder Roy Johannink en communicatieadviseur Charlotte Reddingius waren verantwoordelijk voor de coördinatie van de ROAZ-brede communicatie.

Feiten en cijfers van de ketenoefening cyberaanval

10 ziekenhuizen



5 huisartsenspoedposten

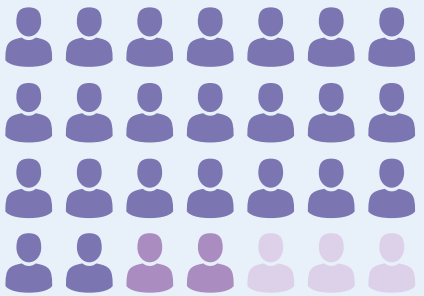
2 RAV'en

3 GGD'en

2 GHOR-bureaus

5 ROAZ-overleggen *

23 oefenleiders zorgorganisaties
02 oefenleiders NAZB
03 oefenleiders COT



26 responscelleden (media en algemeen)

4 nieuwsbrieven

9 WhatsApp-groepen

28 observatoren

450 deelnemers

* DB ROAZ en Tactisch Kernteam (waarin ook VVT, GGZ, revalidatie, dienstapotheek, IGJ en ZV mee-oefenden), ROAZ Ziekenhuizen & RAV, ROAZ Huisartsenzorg, crisiscommunicatie

Ransomware: wel of niet betalen?

De ketenoefening werd op 31 mei afgesloten met een themamiddag waar alle deelnemers voor waren uitgenodigd.

Op de ketenmiddag gaf Joeri Blokhuis (Responders.NU), ethisch hacker en ervaren in onderhandelingen met ransomwaregroepen, een presentatie over hoe het eraan toegaat achter de schermen van ransomware. 'Tijdens de oefening maakten deelnemers mee hoe reëel het is dat een zorgorganisatie om losgeld wordt gevraagd.' Joeri gaf voorbeelden van welke tactieken hackers toepassen om een (zorg)organisatie schaakmat te zetten: phishing, het versleutelen van gegevens, het stelen van gevoelige data en organisaties afpersen om deze data te lekken, het uitvoeren van een DDoS-aanval om het netwerk plat te leggen en bellen naar de klanten van de organisatie om een organisatie onder druk te zetten. Joeri: 'De hackers komen eigenlijk altijd hun afspraken na; dat is het verdienmodel. Hoewel je ze nooit helemaal kunt vertrouwen. Als je alles zelf weer moet opbouwen, kost dat ook heel veel geld. Soms zelfs meer dan de hackers "maar gewoon" te betalen. Natuurlijk brengt dat dilemma's met zich mee. Want je komt wel tegemoet aan de eisen van criminelen. Toch kan een organisatie soms wel besluiten om alsnog te betalen om te voorkomen dat gevoelige informatie op straat komt en mensenlevens in gevaar zijn. Kortom: weeg per situatie af of je wel of niet gaat betalen.' Advies van Joeri is dan ook: 'Zorg zo snel mogelijk voor een goed beeld van de impact van de hack en schakel experts in om je daarin goed te adviseren en begeleiden. Het is vervolgens belangrijk om naar het publiek open en eerlijk te communiceren welke overwegingen er waren om tot een bepaald besluit te komen om wel of niet te betalen.'

Ethisch hacker Joeri Blokhuis geeft een presentatie over ransomware.

Aanbevelingen uit het evaluatierapport

Een ICT-storing/cybercrisis kan de gehele keten raken. Een belangrijk thema dus, net als een pandemie, waar de vorige intersectorale ketenoefening in 2019 op focuste, waarna in 2020 de covidcrisis uitbrak. De vraagstukken en mogelijke dilemma's van een cybercrisis zijn echter anders. De benodigde expertise komt bovendien uit een andere hoek.

Tegelijkertijd zijn er natuurlijk ook parallellen. Een groot deel van de aanbevelingen gaat daarom over ICT-storingen/cybercrises en over crises in het algemeen. Het rapport geeft vier aanbevelingen om de Brabantse acute zorgketen nog beter voor te bereiden op een cyberaanval en/of grootschalige ICT-uitval.

Besteed aandacht aan de structuur, processen en ondersteuning voor de samenwerking tijdens een ketenbrede (cyber)crisis waarbij afstemming in de regio nodig is.

PAST BIJ OEFENDOEL 1 EN 2 >>

Er ligt in Brabant een stevige basis met de ROAZ-structuur. Desondanks is er behoefte aan afspraken die de samenwerking tijdens een crisis ondersteunen. Het COT adviseert:

- Bepaal de uitgangspunten en wederzijdse verwachtingen tussen alle betrokken (cyber)partijen.
- Baken de rollen af. Het ROAZ richt zich op de borging van acute zorg. Ten behoeve van de ICT-storing/cybercrisis, zorg voor een integrale aanpak. Daarbij komen verschillende lijnen samen, denk aan aansluiting vanuit het regionale CISO-overleg op de ROAZ-structuur tijdens de crisis en samenwerken en afspraken maken over rolverdeling met Z-Cert als schakel naar de nationale crisisstructuur.
- Verfijn de rolverdeling tussen GHOR en ROAZ met de focus op samenwerken en met een ondersteunende en coördinerende rol van de GHOR (bijvoorbeeld informatiemanagement (LCMS-GZ)) en de GHOR als schakel naar de veiligheidsregio's. Betrek hierbij de DPG.
- Ondersteuning van het crisisproces. Denk aan specialisten communicatie-, secretaris- en coördinatie die de uitvoer van de samenwerkingsafspraken borgen. Met als hoofdvraag welke verantwoordelijkheid NAZB daarin heeft en wat je realistisch gezien kunt verwachten in termen van middelen, kennis, kunde en capaciteit. Ben daarbij niet alleen afhankelijk van de capaciteit van NAZB; betrek ook reeds opgeleide sleutelrollen van de ketenpartners.
- Verfijnen van het proces van informatie delen.
- Leg kaders en afspraken vast in een Handreiking Regionale Samenwerking tijdens Crises.

Ontwikkel een regionale scenariokaart voor een ICT-storing/cybercrisis.

PAST BIJ OEFENDOEL 1 EN 2 >>

Een scenariokaart is verdiepend op een crisisplan. In de scenariokaart ICT-storing/cybercrisis is in ieder geval aandacht voor:

- concretisering crisis (uitval ICT, ransomware, datalek, datadiefstal);
- uitleg bijzondere impact;
- bijzondere partijen/stakeholders die een rol spelen in het bestrijden van de crisis en hoe zij aansluiten op de crisisstructuur;
- mogelijke kritieke (beslis)momenten;
- gemeenschappelijke doelen (versus organisatiedoelen), uitgangspunten en een afwegingskader voor het omgaan met datalekken, ransomware, afschakelen van ICT;
- afspraken over de communicatie over dit type incident waar het gaat om snelheid, duiding, attributie en samenwerking;
- bijzonderheden van de herstel- en de nafase van een crisis;
- verdere relevante regionale planvorming.

Investeer in de doorontwikkeling van netcentrisch werken.

PAST BIJ OEFENDOEL 1 EN 2 >>

Netcentrisch werken betekent dat alle leden in de crisisorganisatie toegang hebben tot de laatst geverifieerde informatie over het incident en tot een gemeenschappelijk beeld komen en leiding en coördinatie daaraan kunnen koppelen. In Nederland gebruiken we daarvoor LCMS. Een groot deel van de zorgregio gebruikt LCMS-GZ. Het succes van netcentrisch werken staat of valt bij de mate waarin deelnemende organisaties in staat zijn hun eigen beeld bij te houden en te delen, de tijdigheid van een actuele, centrale vertaling van de losse beelden naar één overkoepelend beeld van de situatie en het gemeenschappelijk beeld leidt tot een gedeelde set afspraken die zichtbaar is voor alle deelnemers. Het COT adviseert:

- Ketenpartners zorgen voor opgeleide informatiecoördinatoren, al dan niet gekoppeld aan een bestaande functie, die tijdens een crisis toegang hebben tot de juiste informatie en deze, via LCMS-GZ, met andere ketenpartners kunnen delen. Daarbij is het streven: één werkwijze. Zorg voor een format situatierapportage en verwerk die in LCMS-GZ. Deze rapportages bieden een gemeenschappelijk regionaal beeld.
- Een informatiecoördinator voor de ROAZ-regio. Benut daarvoor de kennis, kunde en capaciteit van de GHOR. Voorwaarde is dat deze informatiecoördinator toegang heeft tot informatie en aanwezig is bij de ROAZ-overleggen.
- Gemaakte afspraken op tactisch en strategisch niveau worden verwerkt in LCMS-GZ, zoals dat tijdens oefening ook gedaan is, zodat alle deelnemende organisaties hiervan kennis kunnen nemen. Alternatieve communicatielijnen anders dan afgesproken worden niet gebruikt.

Blijf werken aan de voorbereiding op crises samen met partners.

PAST BIJ OEFENDOEL 3 >>

De awareness op een ICT-storing/cybercrisis en breder op elk type crisis, is dankzij de ketenoefening vergroot en de behoefte aan samenwerking ook. Om die kennis te behouden, is het belangrijk om regelmatig te blijven oefenen, niet alleen als individuele zorgorganisatie maar ook als keten. Maak op basis van de aanbevelingen een meerjarenontwikkelplan waarin de planvorming en het opleiden, trainen en oefenen, en het evalueren van incidenten een plek krijgt

Hoe nu verder?

Dankzij deze ketenoefening, die als nulmeting diende, ligt er nu een mooie leerlijn voor de toekomst. De komende periode werkt NAZB samen met de ketenpartners en de GHOR aan een handreiking zorgcontinuïteit. Daarin staat omschreven welke doelen, uitgangspunten, communicatie en structuur we gebruiken bij bijzondere omstandigheden, waar het scenario ICT-storing/cyberaanval onderdeel van is. Naast de deelnemende betrokken zorgorganisaties aan deze oefening in mei, betrekken we in de toekomst indien relevant en gewenst ook andere partners en sectoren bij deze planvorming. NAZB houdt de ketenpartners via de ROAZ-overleggen en via de website op de hoogte van de ontwikkelingen.

Samen oefenen, samen leren, samen beter voorbereid

'Samen met Menno Jansen, directeur COT, mocht ik deze bijzondere ketenoefening organiseren, voorbereiden en begeleiden. Als adviseur crisisbeheersing & OTO bij NAZB had ik altijd twee zorgen als het ging om de regionale (acute)zorgcontinuïteit: een pandemie en grootschalige ICT-uitval door cybercriminaliteit. Dankzij de geleerde lessen uit de coronaperiode werden de lijntjes tijdens deze ketenoefening snel gelegd. Dat creëerde veel enthousiasme onder de betrokkenen. Het was spannend om een realistische oefening te creëren met maatwerk voor elke deelnemende zorgorganisatie. De grootte van de organisaties en hun gebruik van digitale systemen varieerden, wat we aanpakten door het scenario langzaam op te bouwen met input van alle organisaties en oefenleiders. Zo werd het scenario realistisch en konden accenten gelegd worden op specifieke onderdelen die elke organisatie wilde beoefenen. De voorbereiding bleek één grote leeractiviteit: wat gebeurt er als een dergelijk scenario werkelijkheid wordt? Met wie heb je dan te maken? Wat mag je doen en wat niet? Dat bood een goede leercurve voor de organisaties en hun interne planvorming. Tijdens de twee oefenochtenden hanteerden we een strakke tijdslijn om het scenario te laten escaleren en input te geven aan de regionale coördinatie. Dat vereiste realistische afwegingen tijdens de ROAZ-overleggen. We ontvingen waarderende feedback over de gekozen dilemma's waarmee deelnemers te maken kregen die zorgden voor nieuwe inzichten. Deze oefening creëerde bewustwording op detailniveau die ons als ROAZ-regio helpt om nog beter voorbereid te zijn.'

Patricia van Roessel
Adviseur crisisbeheersing & OTO NAZB

Adviseurs crisis-beheersing & OTO Patricia van Roessel en Rob van den Bergh (r.), en directeur COT Menno Jansen, tijdens de ketenoefening.

BIJLAGE

Uitdagingen bij een cybercrisis

Deze uitdagingen zijn volgens het evaluatierapport specifiek voor een cybercrisis.

1. Verschillende talen IT/crisismanagement en zorg

Het blijkt lastig om de verschillende betrokken 'werelden' bij elkaar te brengen, mede vanwege de verschillende talen. IT-/cybersecurityspecialisten moeten samenwerken met specialisten zorg, communicatie, crisismanagement, privacy, beleid en operatie. Een uitdaging, zeker omdat de kern van het crisismanagement is dat gezamenlijke duiding plaatsvindt, gewerkt wordt vanuit duidelijke doelstellingen en uitgangspunten, daadkrachtig wordt besloten en dat snelheid wordt gemaakt. In de zorgketen komen die werelden nog niet overal goed bij elkaar.

2. Aansluiting IT bij de crisisstructuur

Het Nationaal CrisisPlan Digitaal beschrijft hoe tijdens een grootschalig cyberincident afgestemd wordt. Hoofden ICT hebben contact met Z-Cert die op zijn beurt afstemt met het National Cyber Security Centrum. Daarnaast zijn diverse betrokken leveranciers, forensische dienstverleners en afnemers samen bezig met het identificeren en oplossen van het probleem. Naar de structuur van de regionale acute zorg is niet automatisch een lijn, waardoor belangrijke informatie over de aard van het incident en een mogelijk verloop van het herstel ontbreken.

3. Voorbereiding verzachtende maatregelen

Afhankelijk van de voorbereiding/inrichting van het systeem bestaan mogelijkheden om na detectie snel verzachtende maatregelen te treffen. Die en andere voorbereidingen zijn direct van invloed op de mogelijkheden voor en snelheid van mitigatie van de impact op zorgcontinuïteit. Niet alle zorgorganisaties hebben hierop al voorbereidingen gedaan.

4. Onbedoeld alerteren kwaadwillenden

Mogelijk is de aanvaller al langere tijd 'binnen' voordat deze wordt gedetecteerd. In de respons moet rekening worden gehouden met het onbedoeld alerteren van kwaadwillenden of het onnodig veroorzaken van onrust. Communiceren over kwetsbaarheden kent risico's: andere kwaadwillen kunnen worden getriggerd om deze kwetsbaarheid in de ICT ook te misbruiken. Dat kan reden zijn om een kwetsbaarheid pas te communiceren als een 'oplossing' is gevonden. Echter, hoe sneller een kwetsbaarheid bekend is bij specialisten, hoe eerder zij maatregelen kunnen treffen.

5. Impact van genomen maatregelen

Naast de impact die een aanval direct kan hebben, wordt de impact bepaald door de respons vanuit de organisatie. Bijvoorbeeld door het uit voorzorg (deels) offline halen van systemen of het niet meer gebruiken van applicaties waardoor zorgprocessen stil komen te liggen. Ook het grootschalig wijzigen van wachtwoorden kan impact hebben op gebruikers. Daarbij speelt het dilemma tussen zorgvuldigheid en snelheid met het oog op zorgcontinuïteit en patiëntveiligheid.

6. Betalen of niet betalen

Ransomware-aanvallen worden geavanceerder en losgeld wordt niet alleen gevraagd voor het ontsleutelen van informatie, maar ook voor het vrijgeven van gevoelige (medische) gegevens. De impact op de bedrijfsvoering en integriteit wordt groter. De kosten voor herstel bij niet betalen zijn hoger dan de kosten voor betaling. Ook als je wel betaalt, zijn de gevolgen vaak een lange onderbreking van ICT door onderzoek, herstel en hoge extra kosten. Het morele kompas bij het betalingsvraagstuk gaat samen met oog voor veiligheid, integriteit en continuïteit. De afweging moet overwogen en navolgbaar zijn en de omgang met de hackers moet in professionele handen zijn. Een goede voorbereiding is cruciaal.

Terug naar inhoudsopgave

Colofon

Redactie NAZB
Fotografie ETZ Fotografie & Film
Vormgeving Anja Verlaat

Augustus 2024

Samen vormen we een stevig netwerk

www.nazb.nl

Netwerk Acute Zorg Brabant

Postadres Postbus 90151, 5000 LC Tilburg
Secretariaat **T** 013 • 221 23 32 **E** secretariaat@nazb.nl