Congres versterkt aandacht en aanpak digitale incidenten in de zorgsector

Goede verbinding tijdens digitale verstoring: punt van zorg?

Digitale verstoringen behoren tot de grootste risico's voor de zorgsector. Het kan namelijk grote gevolgen hebben als bijvoorbeeld dossiers door een stroomstoring, hack of datalek onbereikbaar zijn of juist op straat komen te liggen. Om de bewustwording en kennis over dit thema te bevorderen, bracht het congres ‘Goede verbinding tijdens digitale verstoring: punt van zorg?’ op dinsdag 24 januari 2023 zo’n honderddertig betrokkenen uit de zorgsector bij elkaar. Hoog op de agenda stonden de rolverdeling en samenwerking in de keten.

Het Ministerie van Volksgezondheid, Welzijn en Sport, Traumacentrum Zuidwest-Nederland (bureau ROAZ) en GHOR Zuid-Holland Zuid brachten met het congres medewerkers binnen de zorg bij elkaar die op tactisch en strategisch niveau een rol hebben bij digitale verstoringen. Zoals directeuren, raad van bestuur, zorgmanagers, crisiscoördinatoren, beleidsadviseurs en security specialisten.

Over grenzen

Doelstelling was om over de grenzen van eigen organisaties te kijken, inzichten te delen en gezamenlijk te zoeken naar verbetermogelijkheden en samenwerking. Digitale verstoringen beperken zich namelijk meestal niet tot de grenzen van één organisatie. Incidenten breiden zich vaak als een olievlek uit en maken daarmee samenwerking noodzakelijk.

Digitale incidenten en crises

Dagvoorzitter Chris van ’t Hof stelde bij de start van het congres in Fort Altena in Werkendam dat digitale verstoringen ons allemaal kunnen overkomen. Van Bekende Nederlanders in het ziekenhuis waarbij personeelsleden een ongeoorloofd kijkje in het dossier nemen tot grootschalige hacks.

Chief information security officer Oscar Koeroo van VWS toonde meer voorbeelden. Die maakten duidelijk hoe digitale incidenten kunnen uitgroeien tot omvangrijke crisissituaties. Van eekhoorns en graafmachines die per ongeluk kabels en daarmee internet en telefonie onbruikbaar maken tot een groot incident waarbij in 2021 het Ierse zorgsysteem werd platgelegd en voor tientallen miljoenen euro’s schade werd geleden. In Nederland betaalde een tandartsketen na een cyberaanval in augustus 2022 vermoedelijk twee miljoen euro losgeld aan criminelen.
Koeroo: ‘De zorgsector is veelzijdig maar ook lastig. Want hoe werk je precies samen als verspreid over het land incidenten oppoppen? Als er geen heet water is om te wassen en te

koken, geen stroom om elektrische voertuigen op te laden en om internet en datacenters te laten werken? Zulke situaties zijn moeilijk voor te stellen, maar niet uit te sluiten. Daarom is het goed als we elkaar weten te vinden en op elkaar ingespeeld zijn. We moeten het samen doen.'

Geleerde lessen

Aan de hand van drie presentaties kwamen vervolgens geleerde lessen aan de orde. Zo vertelden Gerda Rodenburg (Traumacentrum ZWN, bureau ROAZ) en Jeroen Peeters (GHOR Zuid-Holland Zuid) over de aandacht die de regio Zuidwest-Nederland het afgelopen jaar besteedde aan digitale weerbaarheid om het bewustzijn van risico's en impact op de eigen instelling en voor de keten te vergroten. Dat gebeurde in Zuidwest-Nederland onder meer met tactische en strategische scenario- en dilemmasessies.

Enkele concrete tips die Rodenburg en Peeters uit de geleerde lessen presenteerden: ken, informeer en help elkaar; spreek bij de planvorming dezelfde taal; besteed in de 'koude fase' aandacht aan scenario-denken, oefenen en beschikbaarheid van communicatiemiddelen; denk in de 'warme fase' aan een brede blik op effecten van de verstoring en snelle inschakeling van hulp.

Voor ondersteuning van organisaties bij hun voorbereidingen op digitale verstoringen hebben zij ook een CrisisToolbox gelanceerd met onder meer een checklist en oefenmogelijkheden.

Samenwerkende Rijnmond Ziekenhuizen testen en oefenen

Dennis Verschuuren (information security officer, Maasstad Ziekenhuis) en Jos Toet (adviseur informatiebeveiliging, Franciscus Gasthuis & Vlietland) lichtten de lessen toe die de werkgroep cybersecurity van de Stichting Samenwerkende Rijnmond Ziekenhuizen leerde. Met de gemeente Rotterdam, politie en Z-CERT (expertisecentrum voor cybersecurity in de zorg) werken zij aan een gezamenlijk regionaal plan. Daarnaast stellen ze een oefenplan op om de werking te toetsen.

Verschuuren vroeg de aanwezigen of hun organisatie zorg kan leveren als internet uitvalt. Een kleine 70% dacht van wel, maar daadwerkelijk getest is er maar weinig. Het Maasstad Ziekenhuis deed dat wel, mede naar aanleiding van de ontwikkelingen in Oekraïne. Het bracht daarbij in beeld waar het ziekenhuis tegenaan loopt als internet meerdere dagen niet beschikbaar is. Verschuuren: 'Medewerkers moesten een drempel over voor deze test, daarom kozen we voor een relatief rustig testmoment. Van 7.00 tot 8.01 uur in een

vakantieperiode. We zijn alle afdelingen van het ziekenhuis nagegaan. In het lab, op de OK, bij de SEH, HR, zorgadministratie en schoonmaak kwam de patiëntenzorg niet in gevaar. Onze analyses vooraf klopten en we kwamen dus aardig door de test heen.' Maar leerpunten waren er zeker. Want bij zo'n oefening weten deelnemers dat alles na een uur weer werkt. Maar wat gebeurt er als internet er drie weken of langer uitligt?

'Na gas, water en licht is informatie eigenlijk onze vierde nutsvoorziening. We gaan ervan uit dat het betrouwbaar is', vulde Toet aan. Maar langdurige uitval is niet denkbeeldig en kan leiden tot opnamestops of verplaatsing van patiënten naar andere instellingen. Ook Verschuuren en Toet onderstreepten hiermee het belang van gezamenlijke voorbereidingen.

Nationaal Cyber Security Centrum ondersteunt

Kees Verkade (adviseur crisisbeheersing Nationaal Cyber Security Centrum, NCSC) ging in op het landelijk beeld van digitale dreiging in Nederland en mogelijkheden om digitale weerbaarheid op regionaal en nationaal niveau te vergroten. 'We zien in de praktijk de gevolgen van cyberaanvallen toenemen. Naar schatting bedraagt de schade wereldwijd 190.000 dollar per seconde', stelde hij. Schade die wordt veroorzaakt door spionage en sabotage, maar bijvoorbeeld ook door beïnvloeding van de verkiezingen in Amerika. Of door hacks. Zo legde een hack in april 2021 een transportbedrijf in Nederland plat, waardoor de kaasschappen bij supermarkten leeg bleven. Voor Verkade is het duidelijk: een fundamentele aanpak is noodzakelijk. Dat betekent voor hem vooral inzicht krijgen in risico's en in zaken binnen jouw organisatie waarin aanvallers het meest geïnteresseerd zijn. En natuurlijk gezamenlijk oefenen. NCSC helpt organisaties op dit vlak door te begrijpen, te verbinden, te voorkomen en tijdens crises te ondersteunen.

Oefenen en samenwerken

In de middag oefenden de deelnemers aan de hand van een fictief scenario van cyber security bedrijf Waker met een incident rondom een EPD/ECD-systeem van een ziekenhuis. Het incident breidde zich uit tot op nationaal niveau en vroeg om steeds omvangrijkere samenwerking. Het is al lastig om overzicht te houden en acties te coördineren bij een verstoring in een enkele organisatie. Verspreiding over meerdere organisaties maakt het alleen maar gecompliceerder, zo maakte ook de oefening duidelijk. Zeker als verschillende regio's betrokken raken die geografisch niet naast elkaar liggen. Want hoe krijg je een beeld van de problemen en wie heb je precies nodig om ze op te lossen? Hoe vind en informeer je elkaar? En zijn de huidige structuren voor crisisbeheersing eigenlijk wel toereikend?

De oefening bood aanknopingspunten om inzichten te delen en gezamenlijk verder te zoeken naar verbetermogelijkheden. Aandachtspunten die de oefenleiders alvast meegaven: wees duidelijk met het plotten van de gebeurtenissen; onderscheid met de BOB-methode de beeld-, oordeels- en besluitvorming; geef duidelijk aan wie welke acties uitvoert; monitor of acties daadwerkelijk worden uitgevoerd; houd elkaar op de hoogte en zorg dat informatie en communicatie twee kanten opgaan.

Leerzaam en enorm nuttig

En de deelnemers, hoe beleefden zij de congresdag? ‘Leuk, leerzaam, lekker interactief, soms chaotisch, maar sowieso enorm nuttig om snel een beeld te krijgen van bedreigingen en mogelijke oplossingen’, waren tijdens de afsluitende borrel reacties op de geboden informatie en de oefening.

De algemene indruk van de deelnemers was dat in ieder geval de IT-kant van organisaties zich bewust is van het feit dat scenario’s weliswaar fictief zijn, maar niet ver afstaan van de realiteit die de zorg kan overkomen. Iets wat een kleine week na het congres nog eens duidelijk werd door een DDoS-aanval van de pro-Russische hackersgroep Killnet op het UMC Groningen. Killnet kiest doelwitten in landen die Oekraïne helpen in de oorlog. Bij de aanval zouden de medische gegevens van patiënten van het UMCG niet in gevaar zijn geweest. Wel werden de homepage, nieuws-, research, en onderwijssites van het ziekenhuis getroffen.

Bij de oefening was het voor sommige deelnemers even zoeken wat wel en niet bij hun rol hoorde. Maar, zo was in de reacties te horen: ‘Het was mooi dat iedereen enthousiast aan de slag ging en dat er ook ruimte was voor een beetje plezier. Zo zijn we op zijn minst weer beter voorbereid op digitale verstoringen en zijn we ons nog meer bewust van het belang van oefenen en samenwerken. Niet alleen binnen individuele organisaties, maar ook op regionaal en landelijk niveau.’

***

GHOR Zuid-Holland Zuid

Ministerie van Volksgezondheid, Welzijn en Sport

ROAZ Zuidwest-Nederland