Verslag kenniskring crisisbeheersing 8 november 2016

Zorgcontinuïteit als een zorgketenpartner tijdelijk uitvalt

Door: Marlène van Vijfeijken | www.cato-communicatie.nl

Wat betekent de uitval van essentiële voorzieningen voor de zorgcontinuïteit in een zorginstelling? En wat betekent het voor de hele zorgketen? Dat waren de centrale vragen tijdens de kenniskring crisisbeheersing die het Netwerk Acute Zorg Brabant (NAZB) op dinsdag 8 november 2016 organiseerde. Vertegenwoordigers van Brabantse zorginstellingen die recent tijdelijk geen zorgcontinuïteit meer konden garanderen, deelden hun ervaringen en geleerde lessen rondom crisisbeheersing.

Is de zorgsector voldoende voorbereid op een moedwillige ICT-uitval?

De samenleving krijgt steeds meer te maken met cybercrime. En dus de zorgsector ook. Voor criminelen zijn data als patiëntengegevens het nieuwe goud. Toch delen zorgverleners deze gegevens regelmatig via onbeveiligde media als WhatsApp, onwetend over de gevaren hiervan. “Op websites zijn medische gegevens te koop voor een gemiddeld prijs van twintig dollar per patiëntendossier”, aldus Krijn de Mik, hoofd Intelligence bij Fox IT. Met zoekprogramma’s als Shodan zoeken criminelen het wereldwijde web af naar apparaten die onbeveiligd aan het internet hangen, stelen de data om die vervolgens voor veel geld te verkopen.

De Mik schetste kort de omvang van het gevaar. Ongeveer vijftig procent van de bedrijven is wel eens gehackt. Meer dan zestig procent had dat zelf niet eens in de gaten en werd daar door externen op geattendeerd. Tachtig procent van de incidenten wordt veroorzaakt door de factor mens. En een virus bevindt zich gemiddeld 177 dagen in een netwerk voordat het wordt ontdekt. “Zo weinig inzicht hebben organisaties dus in hun eigen netwerk.” Het gevaar is zo groot omdat aanvallers uit verschillende hoeken komen, van de zogenaamde scriptkiddies (die voor de lol een programmaatje schrijven om in te breken in een computer en zich niet realiseren wat de impact daarvan is) tot bedrijfsspionage en georganiseerde misdaad.

Uitdaging

Traditioneel hebben organisaties de buitenkant wel goed beveiligd met een firewall. “Maar de zwakste schakel zit in de organisatie zelf: werknemers die een phishing-mail openen en zo allerlei ellende binnenhalen.” Tegelijkertijd bewaren organisaties steeds meer gegevens in de Cloud. “Hoe goed zijn gegevens daar beveiligd?” Ook zijn organisaties zich steeds minder bewust van wat op het eigen netwerk en wat in de Cloud staat. En verliezen dus zicht op de beveiliging daarvan. “Een uitdaging voor de komende jaren”, aldus De Mik.

Zorginstellingen lopen grote risico’s aangevallen te worden. Om de risico’s van cybercrime het hoofd te bieden, moeten ze voorbereid zijn. “Ga er van uit dat je een keer aan de beurt bent”, zegt Martin Zandvliet, expert bij Fox IT. “Komt dan de bedrijfscontinuïteit in gevaar?” Daarom luidt het advies: start detectie, breng risico’s in kaart, creëer awareness en maak het klein: “een olifant eet je in stukjes”. De tien vuistregels voor cybersecurity, een handreiking voor bestuurders en ondernemers kan daarbij als leidraad dienen.

Lessen van ICT-uitval in het Amphia Ziekenhuis

"Ik word niet vrolijk van de vorige spreker", aldus Frank Jaspers, bedrijfsmanager SEH en crisiscoördinator van het Amphia Ziekenhuis. "Want met hacken houden wij als ziekenhuis helemaal geen rekening." Inmiddels wel met datastoringen, want daar had het ziekenhuis dit jaar al drie keer mee te maken. Na twee kleine storingen in april 2016 was het op 10 augustus jl. opnieuw raak. Jaspers vertelde het verhaal van een kortstondig incident dat een grote impact had op het ziekenhuis zelf en op de hele keten.

Sluiting SEH

Het begon op 10 augustus om 18.00 uur met gepland onderhoud aan het rekencentrum. Al snel was het elektronisch patiëntendossier niet meer bereikbaar en vertoonde het hele netwerk storing. Binnen een uur werd het crisisbeleidsteam (CBT) opgestart. Het CBT besloot de SEH te sluiten en op de IC op papier te gaan werken. "We hebben de meldkamer ambulancedienst, de SEH van het Bravis ziekenhuis en het Elisabeth-TweeStedenziekenhuis, de huisartsenpost en de dienstdoende medisch specialisten ingelicht en de technische dienst opgeroepen." Het blijft de hele nacht onduidelijk hoe lang de storing duurt en alle voorbereidingen worden getroffen om het OK-programma van de volgende dag af te zeggen. Uiteindelijk blijkt alles de volgende dag om 8.00 uur stabiel te werken en gaat de SEH weer open.

Lessons learned

Het Amphia Ziekenhuis heeft inmiddels de procedure bij geplande werkzaamheden aan het netwerk aangepast. "We moeten ons ziekenhuisbreed en uniform voorbereiden op de uitval van het digitale netwerk voor als het toch nog fout gaat", concludeert Jaspers. "We moeten in kaart brengen wat we, medisch gezien, nodig hebben om door te werken op de SEH. En hoe lang we dat dan volhouden. Want SEH's sluiten kan echt niet meer." Ook de communicatie naar ketenpartners moet beter. "Er was veel onduidelijkheid over de duur van de storing, wat zij aan extra patiënten konden verwachten en of ze daar extra middelen en mensen op moesten inzetten." Daarom pleit Jaspers ervoor procedures betreffende uitval of sluiting ketenbreed te bespreken. Aan die wens werd meteen gehoor gegeven. "Het Regionaal Overleg Acute Zorg (ROAZ) heeft bepaald dat langdurige ICT-uitval een scenario is waar we de komende jaren met elkaar afspraken over gaan maken", aldus Eelko Netten, adviseur crisisbeheersing & OTO van het NAZB.

Lessen van de brand op de SEH in het Bravis ziekenhuis

Op 12 november 2014 ontstaat rond 10.00 uur forse rookontwikkeling op de SEH van het Bravis ziekenhuis in Bergen op Zoom. Sinds begin 2014 waren er bouwwerkzaamheden op het dak van de SEH, die pas drie jaar in gebruik was. De afdeling wordt ontruimd en de vier aanwezige patiënten worden opgevangen in een vergaderzaal elders in het ziekenhuis. Al snel is duidelijk dat het om een ernstig probleem gaat. De SEH gaat dicht en de patiëntenstroom wordt omgeleid naar de aanstaande fusiepartner in Roosendaal. Het ziekenhuisrampenopvangplan (ZiROP) wordt in werking gesteld en buiten het ziekenhuis wordt een Commando Plaats Incident (CoPI) ingericht. De rook trekt een deel van het ziekenhuis in, waardoor poliklinieken en de ziekenhuisapotheek ontruimd moeten worden. De naast de SEH gelegen huisartsenpost kan om 17.00 uur niet open en verlegt zijn activiteiten ook naar Roosendaal.

Na de brand
Na het sein 'brand meester' zijn alle inspanningen gericht op het zo snel mogelijk heropenen van de SEH. Op 17 november was een beperkt gebied weer in bedrijf, zij het met veel bouw- en andere overlast. "Achteraf gezien hebben we de SEH te snel in gebruik genomen", zegt Petra Verdult, secretaris Raad van Bestuur van het Bravis ziekenhuis. "Medewerkers waren na de ingebruikname redelijk onthand, want niet alle materialen en apparaten waren aanwezig of gecertificeerd. We hebben nu een checklist, zodat een ingebruikname gestructureerd gebeurt."
Ook op andere punten heeft het ziekenhuis lering getrokken uit dit incident. "We hebben de samenwerking met het CoPI en de verplaatsing van de spoedzorg in plannen beschreven. En ook dat het wenselijk is dat een bestuurder op de locatie van de calamiteit aanwezig is."
Leerpunten zijn er ook op het gebied van communicatie. "SEH-medewerkers hadden veel vragen. We hebben die schriftelijk beantwoord. Dat blijkt niet de beste manier. Het is te rationeel, te zakelijk, te weinig oog voor emoties. Ook is het belangrijk dat de Raad van Bestuur zich laat zien in huis, juist in de maanden ná de brand."

Nieuwe SEH
De brand leidde uiteindelijk tot een nieuw crisismanagement- en crisiscommunicatieplan met daaronder een aangepast BHV-plan, een aangepast ZiROP en een nog te maken plan voor datalekken. Maar ook tot een nieuwe SEH "met iets meer kamers dan voorheen en met alle eerdere fouten uit de nieuwbouw hersteld."

Brand in Meander Medisch Centrum
Het Meander Medisch Centrum in Amersfoort werd in januari 2011 getroffen door een brand. Over deze brand, de evacuatie en de terugverhuizing is een film gemaakt.

Discussie: impact (tijdelijke) uitval zorginstelling in Brabantse zorgketen
Uitval van essentiële voorzieningen in zorginstellingen heeft consequenties voor de hele zorgketen. "De aard en omstandigheden zijn bepalend voor de mate van crisismanagement. Maar je kunt beter voor niets of te vroeg opschalen dan te laat of niet, want dan blijf je achter de feiten aanlopen", aldus dagvoorzitter Gert-Jan Ludden.
Voorbereiding op dergelijke uitval is tweeledig. Enerzijds door deze voorzieningen dubbel uit te voeren (noodstroom, back-ups) en door goede servicelevel-agreements af te spreken met leveranciers, anderzijds door het adequaat beoefenen van dergelijke scenario's. "Eén keer per jaar oefenen is geen oefenen. Het hoeft ook niet een hele dag te zijn. Een tabletop van een uurtje of twee is ook prima."

Tot slot
Eelko Netten sloot de bijeenkomst af. "We hopen dat deze bijeenkomst heeft bijgedragen aan bewustwording. Denk na over welke scenario's de meeste impact hebben op de zorg. Wat kunnen we dan doen om in bijzondere omstandigheden als keten toch adequate zorg te verlenen."