Zorg-CERT komt op stoom

Gezamenlijke aanpak van informatiebeveiliging

door: Marcel de Groot

Over informatiebeveiliging in de zorg is al veel geschreven. De oprichting van Zorg-CERT – operationeel sinds juni 2017 – voegt daar nu een belangrijk hoofdstuk aan toe. Zorg-CERT biedt hulp bij cyberincidenten maar bouwt ook kennis en expertise op over digitale veiligheid in de zorg. Deelnemers aan dit initiatief zetten daarom grote stappen in hun weerbaarheid tegen cybercrime.

De Zorg-CERT is een nonprofit initiatief van drie brancheorganisaties: de NFU (De Nederlandse Federatie van Universitair Medische Centra), de NVZ (Nederlandse Vereniging van Ziekenhuizen) en GGZ Nederland. Het ministerie van VWS verstrekte een startsubsidie, die loopt tot medio dit jaar, waarna de Zorg-CERT financieel zelfstandig zal zijn. Over het doel en de activiteiten van Zorg-CERT (Computer Emergency Response Team) spreken we met directeur Nienke van den Berg en David Voetelink, voorzitter van de Raad van Toezicht van de Zorg-CERT. Hij is tevens vice-voorzitter van de Raad van Bestuur van het Rotterdamse Erasmus Medisch Centrum. "Het is niet eenvoudig om de juiste balans te vinden tussen openheid en gastvrijheid van een ziekenhuis als het EMC versus de privacybescherming van patiënten. De Zorg-CERT is een meer dan welkom onderdeel van onze totale patiëntveiligheid. En voor iedere deelnemer vormt het een enorme toevoeging op de eigen securitymaatregelen."

Groei

De eerste doelgroep – categorale instellingen, ziekenhuizen en GGZ-instellingen van de Z-CERT bestaat uit 190 organisaties, waarvan er nu zo'n 50 lid zijn van Z-CERT. Uiteindelijk wil Z-CERT dat alle zorgverleners in Nederland zich aansluiten. Doel is het creëren van een zorgbreed netwerk waarin zorginstellingen, brancheorganisaties, kennisinstellingen, leveranciers enzovoort nauw met elkaar samenwerken, Dit jaar worden pilots gestart voor de volgende doelgroep: langdurige zorg, gehandicaptenzorg en zelfstandige klinieken. "Zo breiden we iedere keer uit", vertelt Van den Berg, "om uiteindelijk vanuit een landelijk netwerk sterker te worden, meer cybersecure. Onlangs is voor de pilot een 'letter of intent' afgesloten met 's Heeren Loo, met een fotomoment en taart. Zij laten daarmee zien dat ze hun informatiebeveiliging serieus nemen, en voor Z-CERT heeft 's Heeren Loo ook een voorbeeldfunctie."

Deelnemersraad

Naast de Raad van Toezicht (zie kader) is er een deelnemersraad die Van den Berg typeert als: "een afspiegeling van de huidige deelnemers. De leden van de deelnemersraad hebben binnen hun organisatie vaak een beleidsmatige rol op het gebied van informatiebeveiliging. Zij adviseren over de dienstverlening van de Zorg-CERT, opdat niet wij als stichting bepalen wat goed zou zijn voor de deelnemers. Die adviezen betreffen niet de specifieke wensen van een aangesloten instelling, maar komen de hele sector ten goede. Alle deelnemers begrijpen dat wanneer één partij binnen de keten (apotheker, psycholoog, een ander ziekenhuis) de informatiebeveiliging niet goed op orde heeft, dit kan terugslaan op anderen. Het helpt niet om naar elkaar te wijzen. Wat wel helpt is het samen oplossen. Dus wanneer de meer volwassen partijen de zwakkere broeders in de keten helpen, helpen ze daarmee uiteindelijk zichzelf."

De inspraak van kleine en grote deelnemers weegt even zwaar in de deelnemersraad.

Voetelink vindt het logisch dat er tussen de diverse zorggebieden verschil bestaat in volwassenheid. "Wij hebben als groot MC nu eenmaal meer middelen dan een klein provinciaal ziekenhuis. Wij hebben er belang bij om iedereen – zeker de instellingen in onze regio – daarin mee te nemen. De CERT hanteert dan ook een groeimodel. Hoe groter de CERT, hoe groter het netwerk dat samenwerkt op het gebied van informatiebeveiliging."

> "Deelnemers maken gebruik van ons internationale netwerk van kennis en expertise"

Hartmonitor

Van den Berg is duidelijk over de adviserende rol van de Zorg-CERT. "Wij nemen niet de verantwoordelijkheid over. Deelnemers maken gebruik van ons internationale netwerk van kennis en expertise. De kwaliteit van de informatie die het netwerk levert, behaal je nooit in je eentje. De Noorse CERT kreeg bijvoorbeeld informatie van een Zweeds ziekenhuis over een haperende hartmonitor. Het apparaat bleef hangen in een rebootloop. Omdat men bang was te zijn gehackt, gaven ze dit aan ons door. Heel snel hoorden we van de Nederlandse leverancier van die monitor dat het een bekende programmeerfout betrof en dat er al een patch was. In vertrouwen kregen wij deze informatie van de leverancier, zodat wij de Noren konden geruststellen dat er geen hack was, maar een relatief onschuldige bug. Nu hoefden ze geen IC's te sluiten en konden wij de Nederlandse deelnemers hierover informeren. Dit bereik je nooit als op zichzelf staande instelling of leverancier."

"Dankzij dit netwerk kan een zorginstelling heel preventief opereren", voegt Voetelink hieraan toe. "Maar het blijft de verantwoordelijkheid van de deelnemer om die patch uit te voeren."

Vertrouwen

Het voorbeeld van de hartmonitor illustreert duidelijk het belang van samenwerking. "Het is in dat kader belangrijk dat ook de leveranciers van medische apparatuur vertrouwen krijgen in de CERT", vertelt Van den Berg. "Zij weten zeker dat informatie onder vertrouwelijkheidsafspraken veilig is en uiteindelijk ook voor hen toegevoegde waarde kan opleveren. Zij horen via ons netwerk heel snel over kwetsbaarheden in hun producten, zodat meteen actie kan worden ondernomen om de schade te beperken. Ook willen wij graag dat netwerken zoals een VECOZO hun kwetsbaarheden aan ons melden. Het incident bij de één is namelijk de waarschuwing voor de ander. Dankzij de melding door een ziekenhuis van een bepaalde phishingmail onlangs, kon eenzelfde incident bij een tweede ziekenhuis tijdig worden ingedamd. Toch kost het winnen van dergelijk vertrouwen tijd. Daarom is het belangrijk om te laten zien dat wij samenwerken met grote professionele partijen."

Voetelink: "De Zorg-CERT is als een brandweer die het liefst preventief opereert. Wij controleren op brandveiligheid, maar bieden ook hulp als de brand eenmaal een feit is. Er loopt nu een groot Actieplan om de bewustwording van onder andere medewerkers te stimuleren, wat ook door VWS wordt gesteund. Daarnaast informeren we op het technische vlak met alerts over verschillende producten, wat er speelt, waar organisaties op moeten letten enzovoort. Dat kan ook algemene informatie zijn, zoals een goed artikel in de media."

Zorginstellingen werken hard aan informatiebeveiliging: bewustwording, beleid, certificering, externe audits enzovoort. "De Zorg-CERT hoort hier gewoon bij", meent Voetelink. "Je hebt straks als zorginstelling iets uit te leggen als je geen lid bent van de Zorg-CERT."

Raad van Toezicht

In de Raad van Toezicht zitten bestuurders van de deelnemende organisaties namens hun branche. Als bestuurder van het EMC hanteert David Voetelink namens de NFU de voorzittershamer. Namens NVZ heeft Hans den Hollander zitting. Hij is bestuursvoorzitter van het Tergooi ziekenhuis en tevens zit er een bestuurslid namens GGZ Nederland in de Raad. Naast deze drie zit ook Elly van den Heuvel, secretaris van de Cyber Security Raad in de RvT. Zij brengt expertise met zich mee op het gebied van cybersecurity én een link naar de politiek. Naarmate de doelgroep van de CERT uitbreidt, zal ook de huidige RvT uitbreiden.