‘Realisatie van een Cybersecurityradar voor Netwerk Acute Zorg Euregio’

Inleiding
Vanuit de regionale Expertgroep Cybercrisis is een opdracht ontstaan voor het realiseren van een Cybersecurityradar. Een Cybersecurityradar dient inzicht te geven in de actuele- en toekomstige dreigingen met betrekking tot cyber-gerelateerde incidenten. Daarnaast is onderzocht wat de kans en impact is op de patiëntveiligheid en (regionale) zorgcontinuïteit. Mart Kemerink, Integrale Veiligheidskunde-student aan Saxion Hogeschool heeft in het kader van zijn afstudeeropdracht dit onderzoek uitgevoerd. De hoofdvraag van het onderzoek luidt als volgt:

‘Op welke wijze kunnen huidige en toekomstige dreigingen, die mogelijk voor een cybercrisis zorgen, gevisualiseerd worden en wat is het verwachte effect, gelet op de patiëntveiligheid en de zorgcontinuïteit binnen het Netwerk Acute Zorg Euregio?’

Samenvatting
In de afgelopen jaren is er veel veranderd op het gebied van ICT in de zorg. Veel zorgprocessen zijn gedigitaliseerd en dat heeft ertoe geleid dat zorginstellingen steeds meer afhankelijk worden van de ICT-voorzieningen. Door de toenemende digitalisering en de gevolgen die daarmee samenhangen heeft Netwerk Acute Zorg Euregio sinds 2018 een regionale Expertgroep Cybercrisis. De expertgroep heeft als doel om de ketenpartners voor te bereiden op een cybercrisis, ook wel digitale ontwrichting genoemd en het managen van de crisis. Vanuit de expertgroep is de vraag ontstaan voor het ontwikkelen van een regionale Cybersecurityradar. Een radar die de huidige- en toekomstige cyberdreigingen en de effecten daarvan, gelet op de patiëntveiligheid en zorgcontinuïteit, in beeld brengt. Het doel van de Cybersecurityradar is om awareness te creëren rondom de relevante dreigingen bij de ketenpartners en draagt het bij aan de informatievoorziening met betrekking tot deze gevaren. Bureau Acute Zorg Euregio heeft eveneens belangen bij het opstellen van een regionale Cybersecurityradar; de radar geeft inzicht met welke gevaren/dreigingen rekening gehouden moeten worden bij het opstellen van het regionaal OTO-jaarplan en uitvoeren van OTO-activiteiten.

Om te bepalen met welke cyberdreigingen rekening gehouden moet worden in Netwerk Acute Zorg Euregio is in het gehele onderzoek gebruik gemaakt van de kennis en kunde van de inhoudsdeskundigen uit de Expertgroep Cybercrisis. De interviews met de experts en literatuurstudie hebben bijgedragen aan het ontdekken van deze relevante gevaren/dreigingen. Vervolgens is onderzocht welke gevolgen de cyberdreigingen met zich meebrengen. Er is onderscheid gemaakt tussen de gevolgen op enerzijds de patiëntveiligheid en anderzijds de (regionale) zorgcontinuïteit. De combinatie tussen enquêtes en literatuurstudie heeft antwoord gegeven op de vorige vraag. Uiteindelijk zijn de relevante cyberdreigingen en bijbehorende gevolgen gevisualiseerd in een welbekend ‘Cybersecurityradar’. Deze radar is exclusief voor Netwerk Acute Zorg Euregio.

Uit het onderzoek is gebleken dat een aantal cyberdreigingen binnen Netwerk Acute Zorg Euregio als relevant kunnen worden beschouwd. Eveneens is vastgesteld dat er nieuwe cyberdreigingen zullen ontstaan waar ketenpartners in de toekomst rekening mee moeten houden. De gevolgen van de cyberdreigingen verschillen onderling, van nauwelijks effecten tot ernstige effecten. Geconcludeerd kan worden dat het leveren van veilige zorg sterk afhankelijk is geworden van een goed werkende ICT. Op basis van het onderzoek zijn aanbevelingen gedaan. Eén van de adviezen is om de Cybersecurityradar te gebruiken bij het vaststellen van de jaarlijkse, regionale OTO-activiteiten.