Blauwdruk over cybersecurity bij ziekenhuizen. Een heldere analyse uit de VS

Op 23 januari 2016 publiceerde het Amerikaanse bedrijf Independent Security Evaluators(IDE) een studie op basis van eigen research over de cybersecurity in de zorg, met name ten aanzien van ziekenhuizen. De titel is "Securing Hospitals". Over dit onderwerp publiceerde ik reeds eerder op 1 februari j.l. en op 18 februari. Het is een kwestie waarvan je op voorhand zou zeggen dat in die sector de computerveiligheid goed geborgd zou moeten zijn, maar niets is minder waar. Regelmatig verschijnen er in de internationale pers berichten over gehackte ziekenhuizen of andere gezondheidszorginstellingen. Het varieert van alleen het aantonen dat hackers in de systemen binnen zijn geweest tot het plaatsen van ransomware. Daarbij versleutelt de malicieuze software van de hacker de programmatuur en data en geeft die pas vrij na betaling van "losgeld". Zoals ik in beide artikelen al verwoordde is er ten aanzien van de cybersecurity in de zorg nog veel te doen. Natuurlijk kan men stellen dat zaken in Nederland anders geregeld zijn dan in de Verenigde Staten, maar de basis van de problematiek is overal hetzelfde.

Onderzoek

Van januari 2014 tot januari 2016 deden wetenschappers, die verbonden zijn aan IDE onderzoek naar de cybersecurity in

twaalf zorginstellingen(voornamelijk ziekenhuizen), twee data-opslagfaciliteiten voor de zorg, twee gecomputeriseerde medisch-diagnostische apparaten en twee webapplicaties. Men nam aan dat hackers en criminelen makkelijk aanvallen ertegen konden lanceren en de gezondheid van de patiënt in gevaar brengen. Binnen die instellingen en bij de fabrikanten van medische apparatuur werd uitgebreid geanalyseerd waar de zwakken plekken in de beveiliging zaten. Ook werd gekeken met "besmette" USB-sticks die met opzet bijv. op het parkeerterrein van de instellingen achter gelaten werden, waar de kwetsbaarheden in de systemen zitten. In de ziekenhuizen werden alle geledingen van die instellingen onder de loep genomen om die uitgebreide analyse te maken. Aan de hand van die analyse werd een uitgebreide blauwdruk gemaakt. Die blauwdruk is een actieplan aan de hand waarvan stapsgewijs het veiligheidsbewustzijn wordt opgevoerd en oplossingen dan wel oplossingsrichtingen worden gegeven voor geconstateerde gebreken.

Rapport

Het 71 pagina's tellende rapport is van de eerste tot de laatste letter uitermate boeiende materie. Grafisch wordt een gedetailleerd aanvalsmodel gepresenteerd in de vorm van een cirkelvormige afbeelding waarin de gehospitaliseerde patiënt centraal staat. De relaties met relevante onderdelen van een ziekenhuisorganisatie worden door middel van sectoren aangegeven. Per sector worden de kwetsbaarheden benoemd en oplossingsrichtingen aangedragen.

Resultaten

In de ziekenhuiswereld is het tamelijk slecht gesteld met de veiligheid van de elektronische systemen door:

- het ontbreken van uitvoerende ondersteuning,
- onvoldoende gekwalificeerd personeel
- onjuiste implementatie van de technologie

- achterhaalde begrip van wat de tegenstander, hacker of crimineel, vermag
- gebrek aan leiderschap,
- een misplaatste vertrouwen op de naleving van regels en procedures

Deze bevindingen bewezen de grote angst van de onderzoekers, te weten: de gezondheid van de patiënt blijkt uitermate kwetsbaar in zorginstellingen door potentiele uitval dan wel malfunctie van elektronische systemen.

Aanrader

Het rapport is een absolute aanrader voor iedereen die in de zorg werkt. Niet alleen het ICT-personeel, maar ook artsen en verpleegkundigen doen er goed aan hun horizon te verbreden. Een groter veiligheidsbewustzijn in zorginstellingen ten aanzien van computers en aan computers gekoppelde apparatuur is geen luxe.

Het is allemaal nodig om dat te doen wat zorgverleners graag willen: goede zorg voor de patiënt.

W.J. Jongejan