Laat cybercriminelen digitale revolutie in de zorg niet verstoren

7 december 2021

Afgezien van het geruststellende regelmatige geluid van de hartmonitor, was het stil in de OK. De steriele ruimte geeft een futuristische aanblik. Schermen, slangen, kabels en apparaten. Hier werken mens en machine samen aan het redden van mensenlevens.

In zijn aanleunwoning zit meneer Jansen aan de koffie. Terwijl hij de krant leest, meet zijn smartwatch zijn bloeddruk en hartslag. Belangrijke data aangezien de heer Jansen een hartpatiënt is. De informatie wordt verzameld in een app die hij aan zijn behandeld arts laat zien bij een eerstvolgende controle.

Ware zorgrevolutie

Wie met een open blik naar de zorg kijkt, ziet in bovenstaande twee voorbeelden dat digitalisering een ware zorgrevolutie teweeg heeft gebracht. Smartwatches meten onze hartslag, slimme systemen waarschuwen je als het tijd is om je medicijnen te nemen en een dwalende alzheimerpatiënt kan op afstand worden gevolgd. Er wordt zelfs gewerkt aan een piepkleine sensor ter grootte van een paracetamol die data verzamelt van het maagdarmkanaal van binnenuit. Makkelijk in te slikken en net zo makkelijk weer uit te scheiden[1].

Die ontwikkelingen maken het werk van zorgverleners en patiënten makkelijker. Ouderen kunnen langer thuis wonen. Chronische zieken krijgen meer invloed op hun leven. Mits goed ingezet kan digitale oplossingen lucht geven in het leven van mensen met een beperking of aandoening. Digitalisering geeft vrijheid, zelfstandigheid, minder pijnlijke ingrepen en uiteindelijk een sneller herstel.

De opmars van digitalisering, in de operatiekamers, in de woonzorgcentra en in de huiskamers is niet van gisteren. Maar het coronavirus heeft die opmars wel in een stroomversnelling gebracht. Zo maakt in 2020 99 procent van de ziekenhuizen gebruik van beeldbellen. In 2019 was dat nog maar 51 procent. Dit blijkt uit een factsheet van de NVZ[2].

Digitalisering zorg zegen

Onlangs vroeg Z-CERT in een online peiling naar wat LinkedIn-volgers vinden van de digitalisering van de zorg. Maar liefst 76 procent is optimistisch en koos voor de derde optie: “Digitalisering in de zorg is een kans.” 17 procent vindt de digitalisering een zegen en slechts 2 procent ziet het somber in en vindt het allemaal maar een nachtmerrie.

Hoewel ver in de minderheid, is het toch 2 procent om rekening mee te houden. Het inzetten van slimme apparaten is mits goed ingezet een prachtige uitvinding, maar risico’s zijn reëel. Los van het feit dat patiënten niet altijd goed weten om te gaan met de slimme systemen, is het geen vervanging van menselijk contact. En dan heb je nog het risico van hackers en digitale verstoringen.

Zorgdomotica kwetsbaar

Wie even online zoekt, vindt tal van voorbeelden waarbij zorgdomotica, ook wel Internet of Medical Things (IoMT) genoemd, kwetsbaar bleek. Ook bij Z-CERT zien we daar elke maand wel een voorbeeld van voorbij komen.

De Amerikaanse website Hipaajournal.com, de onlinebron van berichtgeving over de Amerikaanse AVG (Hipaa (Health Insurance Portability and Accountability Act) publiceerde in 2019 een artikel over een onderzoek naar aanvallen op IoMT-apparaten[3]. Volgens dit onderzoek zou 82 procent van de onderzochte gezondheidsorganisaties te maken hebben gehad met een digitale aanval.

‘39 procent van de respondenten in de gezondheidszorg ziet datalekken als de grootste bedreiging. Aanvallen op IoT-apparaten kunnen ook de patiëntveiligheid in gevaar brengen. 20 procent van de respondenten beschouwde patiëntveiligheid als een groot risico en 30 procent van de zorgverleners die een IoT-cyberaanval hebben meegemaakt, zei dat de patiëntveiligheid daadwerkelijk in gevaar kwam als direct gevolg van de aanval.’ Aldus Hipaajournal.

Kans versus nachtmerrie

Het is een kleine stap van kans naar nachtmerrie. Verstoring van de zorgverlening door slimme zorgapparaten is een serieuze dreiging. Nog niet zo lang geleden moesten honderdduizenden mensen hun pacemaker laten updaten bij hun arts De beveiliging bleek niet op orde. Kwaadwillenden konden op afstand de batterijen sneller leeg laten lopen of zelfs het hartritme van de drager aanpassen. Kwetsbare ICT in je lichaam is wel het laatste waar je op zit te wachten[4].

De grootste nachtmerrie voor elke organisatie, maar voor de zorg specifiek is ransomware. De opmars van de gijzelsoftware waarbij kwaadwillenden systemen ‘gijzelen’ en ze pas weer vrijgeven als er losgeld is betaald, is niet te stoppen. Alleen al dit jaar (tot en met oktober 2021) zijn 33 zorginstellingen in heel Europa geraakt door ransomware. De aanvallen hadden

impact op 66 zorglocaties. Want systemen zijn vaak onderling verbonden.

Feit is, daar waar gedigitaliseerd wordt, zijn kwetsbaarheden en waar kwetsbaarheden zijn, vind je kwaadwillenden die er misbruik van maken. Online criminaliteit is lucratief en de pakkans is nihil.

Angst voor software

Digitalisering is een kans waar we zorgvuldig en verantwoordelijk mee om moeten gaan. Hier houden we ons bij Z-CERT dagelijks mee bezig. Een kwetsbare groep moet zonder angst voor software kwetsbaarheden gebruik kunnen maken van de eindeloze mogelijkheden van de digitalisering. Dat vraagt om een aantal dingen: • Goede begeleiding in het gebruik van (slimme) apparaten, zowel thuis als in de OK. Een slim apparaat is pas echt slim als het slim gebruikt wordt. Wie thuis of in een ziekenhuis op de verkeerde knopjes drukt bij gebrek aan goede instructie, kan schade veroorzaken.

- Een offline back-up voor als de nachtmerrie toch bewaarheid wordt.
- Leveranciers die hun verantwoordelijkheid nemen met veilige producten en het regelmatig updaten van hun producten.
- Een goede samenwerking tussen zorgverlener, patiënt en leverancier.

De zorg is onherkenbaar veranderd in de afgelopen honderd jaar. De ontwikkelingen volgen elkaar in sneltreinvaart op. Laten we ervoor waken dat de cybercriminelen niet in diezelfde vaart de ontwikkelingen verstoren.

Een kwetsbaarheid is snel gevonden

Onderzoekers van security-aanbieder Forescout hebben afgelopen november kwetsbaarheden gevonden in ruim 2.000 medische apparaten zoals anesthesie-apparatuur en patiëntmonitoren. Het gaat volgens expertisecentrum Z-Cert om kwetsbaarheden in het RTOS (realtime operating system) Nucleus NET. Dat wordt gebruikt in diverse medische apparatuur van onder meer Siemens.

De onderzoekers hebben in totaal 5.500 apparaten gevonden die kwetsbaar zijn voor een cyberaanval, waarvan 2.233 gebruikt worden in de zorg – ook in Nederland. Andere dan eerdergenoemde voorbeelden zijn ventilatiesystemen, bloeddrukmeters en infuuspompen. Nucleus software is al bijna dertig jaar in omloop.

Gevaar voor cyberaanval

Kwaadwillenden kunnen deze apparaten aanvallen door misbruik te maken van de kwetsbaarheden. Zo is het mogelijk om gegevens te stelen, de apparatuur uit te schakelen of er op afstand functies van te gebruiken. Z-CERT adviseert gebruikers om contact op te nemen met hun leverancier(s). De instantie stelt de situatie in de gaten te houden en te onderzoeken wat de impact is voor de Nederlandse zorgsector.

Nucleus NET-software wordt in veel sectoren gebruikt, maar vooral toch in de medische sector. Leveranciers die de software gebruiken in hun apparaten zijn op de hoogte gebracht. Siemens heeft een beveiligingsupdate beschikbaar gesteld om deze kwetsbaarheden te verhelpen.

Referenties

1. https://bit.ly/3Cj0PKA
2. https://bit.ly/3kFy0Sx
3. https://bit.ly/2YTiT08
4. https://bit.ly/3DmJMIQ