

Het medische Internet of Things valt of staat met goede beveiliging

29 september 2015



Iedereen hoopt op een lang, gelukkig en vooral gezond leven. Gelukkig heeft de medische wetenschap de afgelopen decennia enorme vooruitgang geboekt, niet alleen op het gebied van geneesmiddelen en behandelmethoden, maar vooral ook in de ontwikkeling van nieuwe medische apparatuur. Deze medische apparaten variëren van relatief eenvoudige apparaten die alleen gezondheid-gerelateerde zaken meten en monitoren, tot systemen die daadwerkelijk levens redden.

Het verzamelen en uitwisselen van kennis en informatie speelt een centrale rol in de verdere ontwikkeling van deze apparaten en in het vergroten van de mogelijkheden ervan. Gelukkig staan we aan de vooravond van een belangrijke volgende stap op het gebied van medische technologie. Ik heb het over 'networked healthcare', of het 'Healthcare Internet of Things'. Dit lijkt sterk op het bekende 'Internet of Things' - een verzameling apparaten die voortdurend met elkaar en met het internet zijn verbonden - maar dan specifiek voor de gezondheidszorg. Dit zal het mogelijk maken om sneller en nauwkeuriger data over onze gezondheid te verzamelen en te analyseren, waardoor nieuwe inzichten ontstaan. Van het medische Internet of Things wordt verwacht dat het ons enorme voordelen gaat opleveren. Het zal ouderen helpen om langer thuis te wonen, zal data opleveren voor nieuwe behandelmethodes en zal - zeker niet onbelangrijk - helpen om de snel groeiende kosten van de gezondheidszorg terug te dringen.

Er zijn al voorbeelden van medische apparaten die dagelijks levens helpen redden of

verlengen. Draadloze implantaten die automatisch insuline inspuiten bij diabetespatiënten. Slimme pacemakers die zorgvuldig afgestemde stroomsignalen geven om het hartritme van patiënten te stabiliseren. Dit zijn slechts enkele bekende voorbeelden. Maar juist omdat ze letterlijk van levensbelang kunnen zijn, is het essentieel om medische Internet of Things-apparaten goed te beveiligen, voordat we de echte voordelen ervan kunnen plukken. De insulinepompen die ik hierboven beschreef, kunnen in theorie op afstand worden gehackt. Ook de pacemaker zou zo geprogrammeerd kunnen worden dat deze het hartritme juist verstoort, met alle gevolgen van dien.

De medische sector als doelwit

Volgens onderzoek vond in 2013 44% van alle geregistreerde data-inbraken in de VS plaats bij bedrijven in de medische sector. Dat is ook niet zo vreemd als we ons beseffen dat medische informatie tien keer zoveel waard kan zijn als bijvoorbeeld creditcardgegevens. Bij Amerikaanse organisaties in de gezondheidszorg is in 2014 de financiële schade ten gevolge van beveiligingsincidenten met 282% toegenomen. Het aantal meldingen van beveiligingsincidenten nam met 60% toe. En slechts 60% van organisaties in de gezondheidszorg heeft hun IoT-apparaten onderworpen aan tests om potentiële risico's vast te stellen. Dat is reden tot 'zorg'.

Er moet nog een hoop gebeuren voordat we alle voordelen van het Healthcare IoT echt kunnen benutten. Een van de belangrijkste stappen is een betere beveiliging. Om te beginnen zou die beveiliging al van meet af aan ingebouwd moeten worden in de apparaten zelf. Medisch professionals kunnen dan zelf eventuele beveiligingsupdates installeren, zodat er niet mee geknoeid kan worden. Daarnaast is het essentieel dat er een betere coördinatie komt tussen publieke en private organisaties in de gezondheidszorg. Door betere samenwerking is het mogelijk om de beveiliging van deze apparaten te verbeteren. Daarnaast moet er ook gekeken worden naar het huidige goedkeuringsproces voor nieuwe medische apparatuur. Het mag niet zo zijn dat een apparaat dat op zeker moment is goedgekeurd, bij iedere beveiligingsupdate het hele (vaak langdurige) goedkeuringstraject opnieuw moet doorlopen. Enerzijds zou dit betekenen dat artsen en patiënten deze belangrijke medische voorzieningen dan langere tijd niet kunnen gebruiken, anderzijds zou dit de fabrikanten ervan kunnen weerhouden om überhaupt beveiligingsupdates uit te brengen.

We hebben nog een flinke weg te gaan voordat het medische IoT goed beveiligd is. Maar het is wel belangrijk dat dit gebeurt. Wanneer technologie op een goede manier wordt ingezet, ben ik ervan overtuigd dat het een belangrijke bijdrage kan leveren aan het verbeteren van de gezondheidszorg. Het Internet of Things kan ons helpen om langer, gezonder en beter te leven. Maar alleen als het ook goed beveiligd is.

Wat dan absoluut helpt is een goed begrip voor deze beveiligingsrisico's bij ziekenhuisbestuurders, naast de focus op medische aspecten en de, soms wel en soms niet accurate, financiële huishouding.

Lees voor meer informatie over dit onderwerp het onderzoeksrapport 'The Healthcare Internet of Things - Rewards and Risks', door The Atlantic Council en Intel Security.

Wim van Campen
VP Noord- en Oost-Europa
Intel Security