Cybersecurity in medische sector: Witte Huis geeft goed voorbeeld

Terwijl enerzijds diverse veiligheidsdiensten in de Verenigde Staten koplopers zijn in het elektronisch afluisteren en volgen van burgers, is daar anderzijds ook een groeiend besef van de kwetsbaarheid van medische apparatuur en hulpmiddelen die aan elektronische ziekenhuisnetwerken gekoppeld zijn. Zeer recent, in januari 2016 werd op initiatief van het Witte Huis, aldaar een ronde tafelgesprek gehouden over cybersecurity in ziekenhuizen en rond elektronische medische apparaten. Eén van de deelnemers, Kevin Fu, professor aan de universiteit van of Michigan en leider van het Archimedes Center for Medical Device Security, bericht hierover op zijn blog. Kevin Fu was ook spreker op de Enigma 2016 conferentie waarover ik recent berichtte in het kader van het risicobewustzijn bij zorgaanbieders ten aanzien van elektronische medische apparatuur Op die bijeenkomst waren naast vertegenwoordigers van de fabrikanten van deze apparatuur ook veiligheidsexperts uit het bedrijfsleven, van overheidsinstanties(waaronder de FBI) en universiteiten aanwezig om te brainstormen over dit onderwerp.

Bijeenkomst

De deelnemers waren bijeen geroepen door de President's Office of Science and Technology Policy (OSTP) en werd geleid door

een tweetal cybersecurity experts van het Witte Huis. Tijdens de sessie werd gesproken over regelgeving door diverse overheids- en gezondheidszorgorganisaties, over bestaande risico's met medische elektronica, over hoe bewust fabrikanten zich zijn van de inbraak- en beïnvloedingsrisico's van de producten die zij maken en met welke inspanningen dat voorkomen kan worden. Professor Kevin Fu was daar vanwege zijn expertise betreffende de veiligheidsissues rond medische elektronische apparatuur en de regelgeving van de Food and Drugs Administration op dat vlak. Bovendien had hij in de jaren 90 van de vorige eeuw in de ziekenhuis ICT-gewerkt en op de werkvloer gezien waar de risico's zich bevinden.

Kevin Fu

Professor Fu sprak op de bijeenkomst desgevraagd over de cybersecurity in ziekenhuizen, over de fabrikanten van elektronische medische apparatuur, over het waarom van de problemen en hoe de diverse stakeholders omgaan met de problemen. Hij vertelde dat het goede nieuws was dat de fabrikanten en ziekenhuizen tegenwoordig serieus geïnteresseerd zijn en naar wegen zoeken de cybersecurity-risico's te beperken. Daarnaast benadrukte hij dat het grootste gevaar op dit moment niet veroorzaakt wordt door high-tech inbraken, maar door niet al te nieuwe huis-tuin- en keuken-malware. Het veroorzaakt tijdelijke uitval van de aangedane systemen vanwege het opruimen van de narigheid en de systemen weer draaiend te krijgen. De verstoring van de patiëntenzorg is dan het grootste probleem Hij had daar uitgebreid over gepubliceerd o.a. in een artikel in de National Academy of Engineering Winter 2015 newsletter en in 2011 in een verslag van een workshop op het Institute of Medicine van de universiteit van Michigan.

Cultuur

Waar hij sterk de nadruk op legde was het belang van het begrijpen van de arbeidscultuur in de ziekenhuizen en andere

gezondheidszorginstellingen. Alle extra ballast die ziekenhuisautomatisering voor de artsen en verpleegkundigen met zich mee brengt, wordt door dezen als hinderlijk ervaren tijdens het werk. Het gevolg is dat iedereen workarounds gaat bedenken om zo min mogelijk last te hebben van de eisen van ICT-ers. Hij hield daarom ook de ICT-mensen een devies voor: “thou shalt not interrupt clinical workflow! Period!”. Let men niet op het verstoren van de dagelijkse routine in ziekenhuizen dan kan met succes met de ICT-plannen wel vergeten. De dokter/verpleegkundige wil de patiënten behandelen en zo min mogelijk last hebben van hinderlijke ICT-zaken. Fu geeft hiermee aan de problemen van de werkvloer even goed te begrijpen als de problemen van het managent en de overheid met de cybersecurity.

Samenwerking

Professor Fu hield ook een krachtig pleidooi richting mede-wetenschappers om uit hun ivoren torens op de universiteit te komen en met de instanties die zich met de cybersecurity bezighouden te werken aan het verminderen van de risico’s. Veel stilzitten is er niet meer bij want in de week voordat Kevin Fu zijn blog schreef(31-01-2016) waren er drie ziekenhuizen door cybersecurity-problemen in de narigheid verdaagd. [a, b, c]. Ook blijken er nu fabrikanten te zijn die nog steeds moeilijk te beveiligen elektronische medische apparatuur maken (remote buffer overflows in drug infusion pumps)

Nederland

De les die uit dit blog en de bijeenkomst waarover die ging in het Witte Huis getrokken kan worden is dat een overheid op goede gronden een samenwerkingsproces kan brengen van werkers in de gezondheidszorg, wetenschappers, fabrikanten en overheidsinstanties om cybersecurity-risico’s tot een aanvaardbaar minimum te beperken. Volledig naar nul terugbrengen is een utopie. De inzet van allen moet niet

éénmalig zijn maar er moet sprake zijn van een permanent proces.

Nederland is elektronisch gezien als het ware de proeftuin van Amerika. Wij scoren met de dichtheid van internet-aansluitingen en computer diensten zeer hoog. Het is een illusie om te denken dat de beschreven problemen hier niet voorkomen. Het volstaat niet met het roepen van ach en wee bij het hacken van ziekenhuizen of dataverlies door criminele oorzaken. Het zou verstandig zijn als de Nederlandse overheid op dezelfde wijze als het Witte Huis de (knappe) koppen bij elkaar zou laten steken in samenwerking met de andere stakeholders op het vlak van cybersecurity in ziekenhuizen en met medische apparaten. In Nederland bestaat sinds 1 januari 2012 het Nationaal CyberSecurity Security Centrum(NCSC), maar het is mij niet duidelijk of het NCSC zich met de hierboven beschreven problematiek zich bezig houdt.

Nog even een aardige anekdote op dit vlak: oud-vice-president Dick Cheney die te boek staat als een “havik” kreeg in 2007 een pacemaker met ingebouwde defibrilaator(ICD) i.v.m. vrij grote hartproblemen. Hij heeft de mogelijkheid om de pacemaker “wireless” te benaderen uit laten zetten omdat hij bang was, op basis van wat wetenschappelijke berichten, dat de pacemaker op afstand door terroristen uitgezet kon worden of kwalijke acties ging uitvoeren

W.J. Jongejan