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

Risicobewustzijn in de zorg

t.a.v. ICT is zorgwekkend: lezing op Enigma 2016 conferentie

Het schort nogal aan het risicobewustzijn in de zorg als het om ICT-gebruik gaat. Dat is de belangrijke boodschap van prof. Avi Rubin op de Enigma 2016 conferentie, die van 25 tot en met 27 januari 2016 in San Francisco voor het eerst werd gehouden. Deze conferentie werd door USENIX, the Advanced Computing Systems Association in de Verenigde Staten georganiseerd. Deze organisatie bestaat sinds 1975 en heeft als doel om ingenieurs, systeembeheerders, wetenschappers en technici, die het neusje van de zalm zijn qua computerkennis en –kunde, bij elkaar te brengen. Elk jaar worden meerdere conferenties gehouden. De Enigma-conferentie is opgezet voor werkers uit de industrie en research om de bedreigingen en cyberaanvallen met een frisse blik gezamenlijk onder ogen te zien. Avi Rubin, hoogleraar computerwetenschappen en directeur van het Health and Medical Security Lab van de John Hopkins Universiteit in Baltimore(VS), hield een fraai betoog over hoe het in grote ziekenhuizen in de VS toegaat in de zorg-ICT. De titel was: “Hacking Health: Security in healthcare IT-systems”” Uit dit verhaal zijn ook lessen te trekken voor de Nederlandse situatie.

Zijn verhaal van rond de 20 minuten staat hier op YouTube.

Risicobewustzijn

Rubin vergeleek de situatie qua risicobewustzijn met diverse andere maatschappelijke sectoren, waarin hij risico-evaluaties had gedaan. In de financiële wereld bleek men de zaken aardig op orde te hebben, in de retail-sector(winkels/supermarkten) was het een stuk slechter, maar in de zorg was het ‘t slechtst ermee gesteld. Aan de hand van een aantal voorbeelden, waarin hij potentiële gevaren en gevaarlijk gedrag identificeert, schetst hij een duidelijk beeld. Eén van de zaken die hem erg verbaasde was het feit dat in de ziekenhuizen vrijwel alle werkers dezelfde toegangsrechten tot medische dossiers hadden. Er was geen duidelijke gelaagdheid aangebracht wie wat mag zien. Ook werd computerapparatuur gebruikt voor doelen waarvoor die niet was bedoeld of aangeschaft.

Gedrag

Daarbij komen aan de orde:

- Workarounds om beveiligingszaken te omzeilen. Op een radiologieafdeling bleek bijv. een personeelslid voor de daar werkzame specialisten de inlog in de werkstations elke 45 minuten opnieuw te verzorgen. De inlogsessies verlipen elke 50 minuten. Door zo te handelen konden de doktoren doorwerken zonder telkens opnieuw zelf in te loggen. Het is te vergelijken met het plakken van post-it-briefjes op beeldschermen met inlogcode en wachtwoord.
- Specialisten logden vanuit huis in via een VPN(Virtual Private Network)-verbinding via het internet op computers/laptops, waar ook hun kinderen spelletjes op speelden etc.

Onderzoeksapparatuur

Niet altijd realiseert men zich dat er steeds meer onderzoeksapparatuur eigen software bevat, die door buitenstaanders aan te vallen is. Te meer omdat die machines gekoppeld zijn met het netwerk van het ziekenhuis.

- Medicatierobots die in de ziekenhuisapotheken de verdeling van de medicatie regelen
- Röntgenapparatuur zoals scanapparatuur
- Bestralingsapparatuur, waarbij complexe doseringsberekeningen uitgevoerd worden.
- Infuuspompen en andere intensive-care-apparatuur
- Bloedanalyseapparatuur in ziekenhuislaboratoria.

Het is geen luchtfietserij, omdat gebleken is dat hackers gericht dit soort apparatuur aanvallen. Medische informatie wordt ook als het nieuwe goud voor criminelen gezien, zelf tien keer waardevoller dan creditcards. Niet alleen kan gedacht worden een het misbruik maken van data die verkregen is, maar ook zogenaamde “ransomware”(tegen betaling weer werking mogelijk maken) kan een organisatie ernstig ontregelen.

Autorun

Apart staat Rubin stil bij de machines op de róntgenafdelingen, die dvd’s branden om het mogelijk te maken bijv. scanonderzoek elders in te zien. Op de dvd’s worden de afbeeldingen gebrand, maar ook een viewer. Dit programma kan met een autorun-programma elders op een computer afgespeeld kan worden ongeacht welk besturingssysteem daarop staat. Het “targetten” van een machine die deze dvd’s maakt in een ziekenhuis, maakt het een hacker mogelijk om via deze weg zeer vele computers elders te besmetten met malware. Gerichte beveiliging van dit soort machines is van groot belang.

Personeelszaken

Ook de computers van de personeels- en managementafdelingen van ziekenhuizen zijn als risico te identificeren bijv. vanwege de consequenties voor de inzet van personeel bij uitval door een cyberaanval van een hacker.

Aparte wereld

Rubin analyseert ook waarom het vaak zo slecht gesteld is met het risicobewustzijn. Hij schetst de ziekenhuiswereld als een omgeving die bevolkt wordt door werkers die hun focus totaal elders hebben liggen en het denken in termen van risico's en beveiliging als een last ervaren bij het behandelen van patiënten. Hij ziet de gezondheidszorg als een unieke sector, waarin veel mensen veel verschillende rollen hebben, met aparte regelgeving. De sector is zeer afhankelijk van software, moet opgeslagen gegevens snel toegankelijk hebben en neigt tot steeds meer gebruik van mobiele apparatuur en gebruik van de cloud. Het bijzondere aan de zorg is echter dat het ons allen aangaat.

10 aanbevelingen

Aan het eind komt hij tot 10 aanbevelingen, die snel zoden aan d dijk zetten, om het risicobewustzijn te verbeteren en tot beter risicogedrag te komen.

- voorkom dat ongeautoriseerde programma's op apparatuur kan draaien(Application whitelisting)
- Zorg voor goede hygiëne ten aanzien van backend-systemen.
- Houdt in de gaten of er geen abnormale zoekopdrachten(queries) gegeven worden
- Zorg voor multi-factor-authenticatie bij toegang van buiten het ziekenhuis.
- Zorg voor toegang via een virtual-machine bij toegang tot klinische data.
- Zorg voor universele versleuteling van data. Bij dataverlies is toegang niet zo maar mogelijk
- Zorg voor goede uniforme afspraken/uniforme juridische regelingen als gebruik wordt gemaakt van opslag in de cloud.
- Beveilig de toegang tot overzichten en tabellen en log de toegang
- Let bijzonder goed op de privacy t.a.v. zelf identificerende uitslagen van onderzoek(DNA, genome-

sequencing)
- Authenticatie van personeel via badges met bepaling wie wat mag doen/inzien.

Het leek mij nuttig deze materie ook een keer hier onder de aandacht te brengen, juist omdat menselijk gedrag universeel is, zeker in de medische wereld.

Wilt u meer zien van Avi Rubin dan is de TEDx-talk van hem uit 2011 ook zeer leerzaam. Die gaat o.a over het hacken van pacemakers, ICD's en auto's.

W.J. Jongejan