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