Hoe cyberinsurance bij kan dragen aan betere ICT-mores in zorgland

Op Twitter verscheen op 2 september 2019 een duidelijke waarschuwing van Matthijs R. Koot, cyberexpert werkzaam bij Secura B.V., een cybersecurity-bedrijf. Het gaat om een zeer recent bekend geworden kwetsbaarheid van bepaalde VPN-diensten, die o.a. in gebruik zijn bij onze overheid en andere instituties. Een kwetsbaarheid die inmiddels hersteld is door een "patch", maar die wel de vraag opwerp of alle gebruikers van VPN-diensten wel adequaat die patch installeren. In zijn blog van 1 september geeft Koot een nauwkeurige beschrijving en wijst daarin een passant op een zeer recent artikel van de juriste Nynke M. Brouwer. Zij werkt als advocaat bij Dirkzwager advocaten & notarissen en als buitenpromovenda verbonden aan het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. Zij publiceerde in het magazine Aansprakelijkheid, Verzekering & Schade, het artikel 'Vlijt en naarstigheid' in een digitale wereld: eigen schuld en beredding in de context van de cyberverzekering' (AV&S 2019/23, afl. 4). Het lijkt een wat droge materie om als niet-jurist te lezen, maar er staan zeer goede observaties en conclusies in. Daarbij denk ik aan hoe in de cyberinsurance verzekeraars bij kunnen dragen aan betere ICT-mores bij hun klanten. Ik kijk in mijn artikel nu naar een deel van die klanten: zorgaanbieders met hun ICT-systemen.

Zeer urgent probleem

Zoals in de aanhef vermeld gaat het probleem met de kwetsbaarheid zeer veel diensten en bedrijven aan. De

kwetsbaarheid zit in Pulse Connect Secure SSL VPN's in de Nederlandse IP-adresruimte. Een anonieme niet-ingelogde aanvaller kan op afstand ermee willekeurige bestanden uitlezen. Er is inmiddels een patch voor. Daarop is echter door nog lang niet alle bedrijven en instituties die gevaar lopen adequaat geacteerd met het installeren van de inmiddels 2 maanden oude patch. In de Nederlandse IP-adresruimte blijkt het om totaal 537 IP-adressen te gaan waarvan er op de ochtend van 2 september 2019 nog 300 kwetsbaar zijn.

Sectoren

De initiële lijst van kwetsbare systemen bevat systemen van:

- Rijksoverheid
- lokale overheden
- luchtvaartsector
- beursgenoteerde bedrijven met intellectual property
- defensie-industrie
- onderwijssector, waaronder een universiteit en een hogeschool
- financiële sector: meerdere banken, verzekeraars, belasting- en administratiekantoren
- ICT-bedrijven: meerdere bekende/grote namen (met o.a. Defensie als klant) en enkele ICT-beveiligingsbedrijven
- havenbedrijven
- petrochemische industrie
- **zorgpartijen: zorgaanbieders en nationale zorg-ICT (WJJ: Ja, welke zouden dat zijn?)**
- enkele kleinere ISPs en telecomproviders
- […meer…]

Actie

Het voorval is gemeld aan cybersecurity-partijen en toezichthouders in Nederland maar het aantal ongepatchte systemen is nog hoog. Op het moment van dit artikel ruim meer dan de helft nog. Bedrijven en instellingen en zeker

zorginstellingen/zorgaanbieders die gebruik maken van VPN-verbindingen dienen zich af te vragen of ze daarvoor Pulse Connect gebruiken en zo ja of de benodigde patch geïnstalleerd is. Indien men wil laten testen of men at risk is kan contact opgenomen worden met matthijs.koot@secura.com van cybersecurity-bedriijf Secura B.V. Door een simpele controle van hostnaam en/of IP/adres kan dan snel een antwoord gegeven worden.

Eigen schuld en bereddingsplicht

Aan de hand van de verzekeringstechnische leerstukken 'eigen schuld' en 'de bereddingsplicht' gaat juriste mr. Nynke Brouwer in haar in de aanhef genoemde artikel diepgaand in op de datgene wat van de klant met een ICT-verzekering en van de verzekeraar verwacht kan en mag worden. Het begrip eigen schuld betekent dat verzekeraars geen schade vergoeden die is veroorzaakt door opzet of roekeloosheid van de verzekerde (artikel 7:952 BW). De bereddingsplicht houdt in dat de uitkeringsplicht van de verzekeraar (mede) bepaald wordt door het handelen van de verzekerde zelf. De verzekerde moet, wil hij recht hebben op (volledige) uitkering voor zijn schade, bijzondere maatregelen treffen om onmiddellijk dreigend gevaar zoveel mogelijk af te wenden of de ontstane schade zoveel mogelijk te beperken.

Cybersecurity

In het artikel maakt Nynke Brouwer duidelijk dat verzekeraars het begrip 'cybersecurity' in vragenlijsten aan klanten en in de te noemen voorwaarden in polisbladen niet eenduidig opstellen. Gezien de voortschrijdende techniek en het bekend worden van nieuwe kwetsbaarheden in hard- en software is het ook lastig om tot in detail de te nemen maatregelen vast te leggen.

Constatering

Brouwer constateert op pagina 122 van haar artikel:

Een enkele uitzondering daargelaten, worden deze maatregelen echter weinig geconcretiseerd. Binnen hoeveel dagen een patch of update moet worden geïmplementeerd, is dus aan de inschatting van de verzekerde zelf. Ik vraag mij af of dit niet een gemiste kans is voor zowel verzekeraars zelf als de maatschappij in bredere zin. Grote incidenten zoals Wannacry en NotPetya tonen aan dat het belang van zo snel mogelijk patchen zeker niet moet worden onderschat. Ter verhindering van de kwetsbaarheid die Wannacry mogelijk maakte had Microsoft al twee maanden eerder een patch uitgegeven, maar nog niet alle bedrijven en organisaties hadden deze geïnstalleerd. Dit lijkt vrij eenvoudig te ondervangen door in de polisvoorwaarden of – zou dit meer maatwerk betreffen – op het polisblad een termijn voor het installeren van patches op te nemen. Hetzelfde geldt voor de algemeen gestelde vraag naar back-ups. De aanvraagformulieren geven niet aan hoe vaak deze back-ups moeten worden gemaakt en waar dat wel het geval is, zijn de verschillen groot: dagelijks, wekelijks, maandelijks.

Disciplinerend

Waar in zorginstellingen het regelmatig installeren van updates en patches van de software nogal eens het stiefkind is, kunnen cyberverzekeraars een broodnodige disciplinerende werking gaan hebben op het gedrag van verzekerden. Geen uitkering van de verzekering bij cybercalamiteiten als de zorgverlener/ zorginstellingen niet aan zijn zorgplicht ten aanzien van de eigen hard- en software heeft voldaan. Kortweg dus: wie klant is bij een cyberverzekeraar en vier maanden lang een kritieke beveiligingspatch op een internet-facing systeem niet installeert hoeft bij een compromittering waarschijnlijk niet te rekenen op een uitkering. De in dit artikel genoemde kwetsbaarheid met Pulse connect Secure SSL

VPN is daar een voorbeeld van.

Het zou een welkome vorm zijn van het brengen van druk op de ketel zijn.

W.J. Jongejan, 3 september 2019

Afbeelding van Andrew Martin via Pixabay

Medtronic roept insulinepompen terug vanwege kwetsbaarheden

Op 28 juni 2019 berichtte het online magazine www.theregister.co.uk een bericht over zeer recent ontdekte elektronische kwetsbaarheden. Het artikel, genaamd "Scumbags can program vulnerable Medtronic insulin pumps over the air to murder diabetics – insecure kit recalled" beschrijft de terugroepactie van het Amerikaanse bedrijf Medtronic van bepaalde typen insulinepompjes. Die bleken kwetsbaar voor beïnvloeding met radio-frequente signalen. Potentiële aanvallers kunnen met speciale technische vaardigheden en dito uitrusting contactloos van een in de buurt zijnde insulinepomp de instellingen veranderen en daarmee de insuline-afgifte beïnvloeden. Het gaat om de MiniMed 508 en de MiniMed Paradigm pompen. De Minimed 620G, 630G, 640G en 670G hebben die kwetsbaarheden niet. Het bedrijf Medtronic heeft in de Verenigde Staten aan gebruikers aangeboden de kwetsbare typen om te ruilen tegen de MiniMed 670G. Voor de duidelijkheid zij opgemerkt dat cybersecurity-onderzoekers de kwetsbaarheden

ontdekt hebben, maar dat er geen tekenen zijn dat daadwerkelijke kwaadwillige beïnvloeding heeft plaatsgevonden.

Probleem

Het probleem zit hem in de draadloze verbinding die bestaat tussen de kwetsbare inulinepompen en CareLink-software. Daarmee kan de informatie van patiënten via hun diabetesapparaten verzameld worden verwerkt worden en omgezet worden in grafieken en tabellen. Daardoor krijgt de patiënt een beter zicht op zijn ziekte. Een aanvaller die fysiek voldoende dichtbij is, kan zich elektronisch voordoen als een CareLink-apparaat. Dan kan die een potentieel levensbedreigend commando naar de insulinepomp sturen. Door de pomp meer insuline te laten toedienen dan nodig is kan een levensbedreigende bloedsuikerdaling op gang gebracht worden.

Research

De kwetsbaarheden zijn ontdekt door een drietal externe cybersecurity-onderzoekers, Rios, Butts en Young die voortborduurden op eerder onderzoek van een groepje andere onzerzoekers(Paul, Radcliffe en Jack). Medtronic heeft het werk van de onderzoekers geverifieerd en aanvullend onderzoek gedaan en meldde het zelf in de V.S. aan de verantwoordelijke organisatie, de National Cybersecurity & Communications Integration Center (*NCCIC*).

Waarschuwingen

Daarna kwamen de waarschuwingen op gang. De kwetsbaarheid is gerubriceerd als CVE-2019-10964. Op de lijst van Common Weakness Enumerations staat het te boek onder de rubriek Improper Access Control. Ook bij het CyberInfrastructure Agency staat het beschreven.

Medtronic

Het bedrijf heeft een bulletin uitgegeven over dit onderwerp. Het biedt zoals eerder gezegd de klanten in de V.S. aan om kwetsbare apparaten om te ruilen voor de MiniMed 670G. voor klanten buiten de V.S. geeft de firma aan dat die een brief zullen ontvangen met instructies die afhankelijk zijn van het land van herkomst. Men raadt de patiënten aan met hun zorgverleners dit probleem te bespreken en te bediscussiëren welke cybersecurity-maatregelen genomen kunnen worden om zich te beschermen. In landen waar geen nieuwer model pomp beschikbaar is raadt de firma aan om veiligheidsmaatregelen in acht te nemen die het in het persbulletin beschrijft.

Voorzorgen

Men raadt aan:

- Houdt de insulinepomp en de daarmee verbonden apparatuur te allen tijde onder eigen controle.
- Bewaar het serienummer van de pomp op een veilige wijze/plaats.
- Let goed op meldingen, alarmen en waarschuwingen van de pomp.
- Stop/onderbreek alle niet bedoelde bolussen van insuline met de pomp.
- Houdt de bloedsuikerspiegel goed in de gaten handel dienovereenkomstig.
- Verbindt de pomp niet apparaten en gebruik geen software die niet goedgekeurd zijn door Medtronic.
- Ontkoppel elk apparaat met CareLink-software als het niet gebruikt wordt om data van de pomp te downloaden.
- Roep medische hulp in als je symptomen van ernstige hypoglycaemie ondervindt of van ketoacidose. Of als je ontdekt dat de instellingen van de insulinepomp of de insuline afgifte onverwachts veranderd zijn.

Kwetsbaar

Elektronica heeft ons in de zorg veel revolutionaire veranderingen gebracht. Daar is de insulinepomp er één van, samen met het relatieve gemak van het bepalen van de bloedsuikerconcentratie in het bloed door de patiënt. Voornoemde kwetsbaarheden laten zien dat we continu ook alert moeten zijn op de gevaren die verbonden zijn met deze apparatuur.

W.J. Jongejan, 1 juli 2019

Crimineel verkregen elektronisch medisch dossier tussen 250 tot 1000 dollar waard

Op 11 april 2019 publiceerde het Department of Health and Human Services (HHS) een kennisgeving over cybersecurity in de zorg. Dit departement van de V.S. is de tegenhanger van ons ministerie van VWS. De publicatie, bestaande uit 13 sheets, is een briefing met als titel "Dark Web PHI Marketplace". PHI staat voor Protected Health Information. In de publicatie wijst het ministerie op de enorme consequenties van het illegaal verwerven en verhandelen van crimineel verkregen

zorgdata op het schimmige deel van het internet, het Dark Web. Daarop is het mogelijk dat kwaadwillende personen/organisaties illegaal verkregen zorgdata kopen en verkopen die afkomstig zijn van datalekken. Dat soort marktplaatsen stimuleren cybercriminelen om zorgorganisaties elektronisch aan te vallen en de buit te gelde te maken. Zorgdata zijn volgens het ministerie op dit moment één van de meest winstgevende data op het Dark Web. Criminelen kunnen daar anoniem acteren zonder angst voor repercussies.

Waar is het om te doen?

Het gaat criminelen om het verkrijgen van tot een persoon herleidbare informatie (Personally Identifying Information (PII). Niet alleen zorgdata staan in de belangstelling maar ook social media accounts, onderwijsbestanden en bestanden uit gemeentelijke administraties. Zorgdata staan speciaal in de belangstelling, omdat daar een scala van criminele activiteiten mee uit te voeren zijn. Dat met een lager risico dan als het gaat om financiële data. Fraude met zorgdata is moeilijker te achterhalen dan financiële fraude bijv. met creditkaarten. Met informatie uit zorgdossiers zijn meerdere typen fraude uitvoerbaar.

Wat gebeurt ermee?

Grofweg kan men het misbruik in vier categorieën indelen.

1. Diefstal van de medische identiteit. Met iemands medische gegevens probeert men medische diensten te verkrijgen: voorschriften voor medicatie(opiaten bijv.), medische ingrepen, valse verzekeringsclaims
2. Financiële fraude met gebruikmaking van tot een persoon herleidbare informatie bij banken en creditcard-maatschappijen. Medische dossiers bevatten namelijk vaak informatie over betaalwijze, bankgegevens etc.
3. Gebruik maken van gevoelige zorgdata om individuen te

bedreigen, af te persen of te beïnvloeden. Daarbij kan het om echte buitgemaakte data zijn, maar ook gemanipuleerde data. VIP’s en bekende publieke personen zijn extra kwetsbaar.
4. Buitgemaakte data kunnen gebruikt worden bij verder gaande cyberaanvallen, bijv. met behulp van phishing mail en vormen van oplichting. Ook kan informatie gebruikt worden om nieuwe aanvallen uit te voeren met buitgemaakte toegangs-/authenticatie-informatie.

Waarde

Het Department of HHS schat de waarde van zorgdossiers op het Dark Web **op 250 tot 1000 dollar per dossier.** De waarde is zo hoog omdat zorgdossiers vaak persoonsgegevens, financiële gegevens en medische data in een compacte vorm bevatten. In de zorg gebruiken we in Nederland het BurgerServiceNummer(BSN), waarmee ook identiteitsfraude uitgevoerd kan worden.

Kwetsbare groepen

In de publicatie noemt het departement drie specifieke groepen, waarvan de gegevens extra interessant zijn voor de criminelen.

- **Jonge kinderen**. Bij data, afkomstig van hacks, is op het Dark Web vooral de “versheid” van belang, d.w.z. dat de data niet eerder gebruikt zijn voor fraude. Data van jonge kinderen zijn dan ook “vers” te noemen. Ze kunnen gebruikt worden voor kredietaanvragen, grote aankopen, zonder dat het slachtoffer er erg in heeft. In de V.S. zijn er onvoldoende controlemechanismen om misbruik van de identiteit van een kind bij kredietfraude op te sporen.
- **Ouderen.** Daarbij speelt financiële kwetsbaarheid die geassocieerd is met de leeftijd. De Federal Trade Commission, een onafhankelijk agentschap van de Amerikaanse federale overheid, schat dat 35% van de

klachten over fraude en 19% van de identiteitsdiefstal bij 65 plussers zich voordoet.

- **Overledenen.** Het is gebleken dat criminelen de gegevens van overledenen als “veiliger” zijn gaan beschouwen naarmate de bewustwording van fraude bij de burger stijgt. De identiteit van overledenen blijkt gebruikt te worden bij creditcard-fraude, belastingfraude en de aankoop van dure artikelen.

Bewustwording

Het Department of Health and Human services beoogt met de publicatie een grotere bewustwording voor de problematiek bij zorgorganisaties,zorgverleners en bij burgers. Cybersecurity is van groot belang bij zorgverleners en in zorginstellingen. Veel meer dan voorheen zal men zich bewust moeten zijn van de manier waarop bedreigingen zich voordoen. Net zoals bij steriliteit is het bij het gebruik van digitale middelen een goede “hygiene” van groot belang. Niet alleen van de ICT-ers die in de zorg werkzaam zijn, maar vooral van de werkers zelf. Een goed voorbeeld van alerte werknemers is bijvoorbeeld de community “Women in Cybersecurity”.

W.J. Jongejan, 21 mei 2019

Ongeautoriseerd inzien

zorgdata soms vanuit zeer onverwachte hoek

Niets is wat het lijkt te zijn. Deze nogal cynische uitdrukking is helaas vaak van toepassing, zeker in de ICT-wereld. In The Wallstreet Journal van 19 april 2017 stond een schokkend artikel over een Amerikaans IT-beveiligingsbedrijf, Tanium genaamd. Het bedrijf heeft toekomstige klanten gedurende enkele jaren de mogelijkheid geboden live in het netwerk van ziekenhuizen te kijken en heeft ook video's daarvan op YouTube gezet. Dat alles zonder dat de ziekenhuizen daar toestemming voor gaven. Terwijl het artikel in The Wallstreet Journal achter een betaalmuur zit, is er toch berichtgeving hierover die vrij te volgen is. De zaak kwam aan het rollen toen het El Camino ziekenhuis in Santa Clara County in Californië erop attent werd gemaakt dat 15 seconden durende filmpjes op YouTube te zien waren met informatie van het managementsysteem van het ziekenhuis. De ziekenhuisdirectie was hoogst verbaasd en verontwaardigd dat de leverancier van de software, die ze in 2010 aanschafte, minimaal gedurende vijf jaar deze vreemde handelswijze heeft gebezigd. Dat het om die jaren gaat blijkt uit de datering van de enkele honderden filmpjes op YouTube, die overigens inmiddels allemaal verwijderd zijn. De filmpjes waren ook te zien op het bedrijfsnetwerk van het cybersecurity-bedrijf.

El Camino Hospital

Het ziekenhuis heeft laten weten dat ze niet op de hoogte waren van dit gebruik van hun data en nooit toestemming gaf voor enige verkooppresentatie. Het ging om management informatie van het ziekenhuis, maar nooit om directe patiënteninformatie, benadrukt men. EL Camino Hospital is duidelijk not amused. Het ziekenhuis heeft inmiddels laten weten dat haar relatie met Tanium beëindigd zijn vanwege deze kwestie. Wat de software van het bedrijf deed, staat bekend als zogenaamde endpoint-security. Daarbij gaat het er om dat de software er voor zorgt dat alle PC's, smartphones, tablets en andere aan het ICT-systeem te koppelen apparaten de meest recente updates van programmatuur hebben, veilig zijn en niet te gebruiken als toegangspoort voor hackers. De binnendringers kwamen echter van een tegenovergestelde richting. In een artikel in de Business Insider staat een leuke vergelijking met een conciërge van je kantoor die allerlei onbekende lieden je bedrijfsruimtes laat zien om aan te tonen hoe goed hij het pand bewaakt.

Verdediging

Inmiddels heeft de topman van Tanium, Orion Hindawi, een verklaring uitgegeven die op zich weer veel bevreemding wekt. In die verklaring geeft hij aan dat enkele klanten geen bezwaar hebben tegen het verzorgen van demo's met hun bedrijfsgegevens. Die toestemming zou dan schriftelijk vastgelegd zijn. Gezien de gevoeligheid van bedrijfsgegevens op managementniveau verbaast deze uitspraak al. Hij vervolgt met de opmerking dat er in het specifieke geval met het EL Camino Hospital zonder toestemming gebruik gemaakt is van een demo-omgeving bij de klant. De IT-afdeling van het ziekenhuis zou met gebruik van fictieve data een demonstratie-database met gegevens hebben aangemaakt om dingen uit te testen met de leverancier of voor instructie aan eigen personeel. Hiermee suggereert hij dat de IT-afdeling van het ziekenhuis dit gebruik mogelijk zou hebben gemaakt en goedgekeurd. Het ziekenhuis heeft in een reactie echter laten weten nooit

geweten te hebben wat Tanium aan het doen was en nooit toestemming gaf om enig materiaal te laten gebruiken voor verkoopuitingen van Tanium.

Moraal

Wat van deze casus te leren is dat gevaren in (zorg)ICT-land niet altijd uit de hoek komen van waaruit je ze verwacht. Kortzichtige beslissingen bij een leverancier bedoeld voor winst op de korte termijn kan het vertrouwen met de klanten op de lange termijn ernstig schaden. Het verdient daarom aanbeveling altijd kritisch te blijven tegenover de eigen ICT-leveranciers en alert te reageren op vreemde gebeurtenissen met of rond de software die ze leveren.

W.J. Jongejan

Blauwdruk over cybersecurity bij ziekenhuizen. Een heldere analyse uit de VS

Op 23 januari 2016 publiceerde het Amerikaanse bedrijf Independent Security Evaluators(IDE) een studie op basis van

eigen research over de cybersecurity in de zorg, met name ten aanzien van ziekenhuizen. De titel is "Securing Hospitals". Over dit onderwerp publiceerde ik reeds eerder op 1 februari j.l. en op 18 februari. Het is een kwestie waarvan je op voorhand zou zeggen dat in die sector de computerveiligheid goed geborgd zou moeten zijn, maar niets is minder waar. Regelmatig verschijnen er in de internationale pers berichten over gehackte ziekenhuizen of andere gezondheidszorginstellingen. Het varieert van alleen het aantonen dat hackers in de systemen binnen zijn geweest tot het plaatsen van ransomware. Daarbij versleutelt de malicieuze software van de hacker de programmatuur en data en geeft die pas vrij na betaling van "losgeld". Zoals ik in beide artikelen al verwoordde is er ten aanzien van de cybersecurity in de zorg nog veel te doen. Natuurlijk kan men stellen dat zaken in Nederland anders geregeld zijn dan in de Verenigde Staten, maar de basis van de problematiek is overal hetzelfde.

Onderzoek

Van januari 2014 tot januari 2016 deden wetenschappers, die verbonden zijn aan IDE onderzoek naar de cybersecurity in twaalf zorginstellingen(voornamelijk ziekenhuizen), twee data-opslagfaciliteiten voor de zorg, twee gecomputeriseerde medisch-diagnostische apparaten en twee webapplicaties. Men nam aan dat hackers en criminelen makkelijk aanvallen ertegen konden lanceren en de gezondheid van de patiënt in gevaar brengen. Binnen die instellingen en bij de fabrikanten van medische apparatuur werd uitgebreid geanalyseerd waar de zwakken plekken in de beveiliging zaten. Ook werd gekeken met "besmette" USB-sticks die met opzet bijv. op het parkeerterrein van de instellingen achter gelaten werden, waar de kwetsbaarheden in de systemen zitten. In de ziekenhuizen werden alle geledingen van die instellingen onder de loep genomen om die uitgebreide analyse te maken. Aan de hand van die analyse werd een uitgebreide blauwdruk gemaakt. Die blauwdruk is een actieplan aan de hand waarvan stapsgewijs het

veiligheidsbewustzijn wordt opgevoerd en oplossingen dan wel oplossingsrichtingen worden gegeven voor geconstateerde gebreken.

Rapport

Het 71 pagina's tellende rapport is van de eerste tot de laatste letter uitermate boeiende materie. Grafisch wordt een gedetailleerd aanvalsmodel gepresenteerd in de vorm van een cirkelvormige afbeelding waarin de gehospitaliseerde patiënt centraal staat. De relaties met relevante onderdelen van een ziekenhuisorganisatie worden door middel van sectoren aangegeven. Per sector worden de kwetsbaarheden benoemd en oplossingsrichtingen aangedragen.

Resultaten

In de ziekenhuiswereld is het tamelijk slecht gesteld met de veiligheid van de elektronische systemen door:

- het ontbreken van uitvoerende ondersteuning,
- onvoldoende gekwalificeerd personeel
- onjuiste implementatie van de technologie
- achterhaalde begrip van wat de tegenstander, hacker of crimineel, vermag
- gebrek aan leiderschap,
- een misplaatste vertrouwen op de naleving van regels en procedures

Deze bevindingen bewezen de grote angst van de onderzoekers, te weten: de gezondheid van de patiënt blijkt uitermate kwetsbaar in zorginstellingen door potentiele uitval dan wel malfunctie van elektronische systemen.

Aanrader

Het rapport is een absolute aanrader voor iedereen die in de zorg werkt. Niet alleen het ICT-personeel, maar ook artsen en verpleegkundigen doen er goed aan hun horizon te verbreden.

Een groter veiligheidsbewustzijn in zorginstellingen ten aanzien van computers en aan computers gekoppelde apparatuur is geen luxe.

Het is allemaal nodig om dat te doen wat zorgverleners graag willen: goede zorg voor de patiënt.

W.J. Jongejan

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