Deloitte.

Cyber security van netwerk verbonden Medische Apparatuur in Nederland 2015

Risico's en good practices voor een weerbare zorgsector

Ir. Jeroen Slobbe
Tel: +31 88 288 27 53
E-mail: jslobbe@deloitte.nl

Contents

Inleiding

Sinds het rapport van de Amerikaanse 'Government Accountability Office' (GAO) over het hacken van medische apparatuur is verschenen, neemt de aandacht voor dit onderwerp toe. Omdat dit rapport veelal Amerikaans onderzoek betreft, heeft Deloitte het initiatief genomen om in Nederland de staat van de beveiliging van medische apparatuur in ziekenhuizen te peilen.

Tussen eind 2013 en begin 2015 spraken we met 17 van de 82 Nederlandse ziekenhuizen over de cyber security van medische apparatuur. We interviewden Hoofden Medische Technologie, Hoofden IT, (Chief) Information Security Officers, Privacy Officers, specialisten en artsen die binnen de ziekenhuizen verantwoordelijk zijn of werken met medische apparatuur.

De trendobservatie dat steeds meer medische apparatuur een netwerkaansluiting heeft, wordt breed gedragen door de ziekenhuizen. Te denken valt hierbij aan hartmonitoren, infusie-apparatuur en MRI-scanners. Door de toegenomen connectiviteit ontstaan dreigingsscenario's die de patiëntveiligheid direct kunnen raken. Voorbeelden hiervan zijn:

- Een patiënt ontvangt geen therapie doordat een signaal van een apparaat wordt geblokkeerd terwijl hij wel therapie nodig heeft;
- Een patiënt ontvangt therapie doordat een hacker hiertoe opdracht heeft gegeven, terwijl hij deze therapie niet nodig heeft;
- Een patiënt ontvangt therapie van een apparaat waarbij een hacker de instellingen heeft aangepast. Hierdoor ontvangt de patiënt andere therapie dan hij nodig heeft;
- Een alarm gaat af doordat een hacker hiertoe opdracht geeft terwijl het alarm niet af moet gaan. Hierdoor kan alarmmoeheid optreden en kan de verpleegkundige tijdelijk geen echte alarmen beantwoorden;
- Een alarm gaat niet af doordat een hacker dit actief blokkeert terwijl het alarm wel af moet gaan (beschikbaarheid).

In dit rapport bespreken we de resultaten van de interviews en presenteren we de lessons learned en good practices die we in het afgelopen jaar hebben opgedaan. Wij hopen dat u hiermee tot nieuwe inzichten komt en met ons de volgende stappen neemt in het beveiligen van medische apparatuur tegen cyberdreigingen.

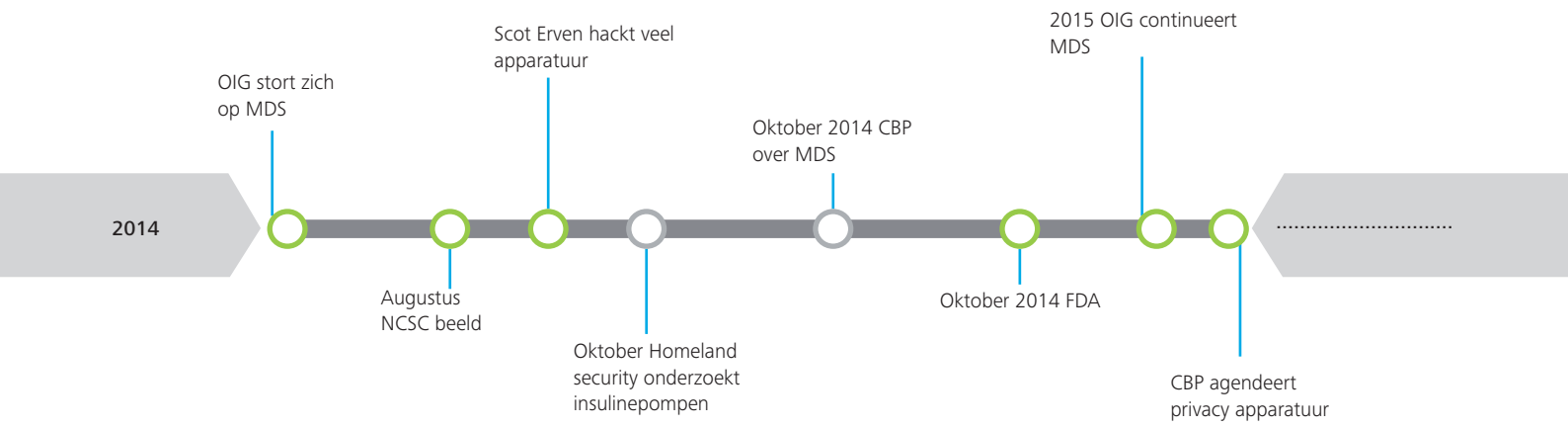
Aanpak

Onder de belofte van strikte anonimiteit hebben we 17 interviews afgenomen bij verschillende ziekenhuizen in Nederland. Deze ziekenhuizen verschillen van elkaar in omvang, locatie en type (algemeen/academisch). We zijn in een tijdspanne van anderhalf jaar het gesprek aangegaan met diverse professionals uit het ziekenhuis die veel met medische apparatuur en/of IT te maken hebben. Voordat het vraaggesprek plaatsvond, kregen de professionals een presentatie over de risico's die beschreven staan in de literatuur en de onderzoeken die in Amerika hebben plaatsgevonden. Daarna volgde een uitgebreid vraaggesprek met het ziekenhuis.

Na een zorgvuldige controle door het Deloitteteam, om te waarborgen dat de antwoorden juist geformuleerd waren, zijn de gegevens tot statistieken verwerkt.

Gebeurtenissen in 2014 rondom de beveiliging van medische apparatuur

Waar in 2013 veel apparatuur werd gehackt, was 2014 het jaar dat overheidsinstanties Medical Device Security in het vizier kregen. Zo stortten de Office Inspector General (de Amerikaanse Inspectie Gezondheidszorg), Homeland Security, de FBI en de FDA zich op deze nieuwe technologie en bijbehorende risico's. In Nederland werd cyber security van medische apparatuur als dreiging aangemerkt in het cyber security beeld van het Nationaal Cyber Security Center. Ook het College Bescherming Persoonsgegevens gaf aan dat medische apparatuur die is aangesloten op het netwerk over adequate beveiliging dient te beschikken. Daarnaast maakte Hollywood gretig gebruik van scenario's. In onder andere de series 'Homeland' en 'Person of interest' werden personages gehackt en beschadigd.



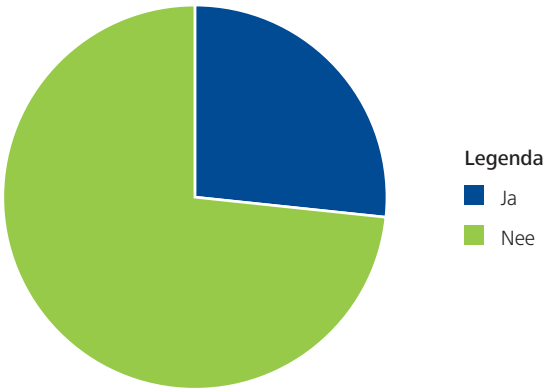
Alle geïnterviewde ziekenhuizen gaven aan een duidelijke trend te zien in de netwerkmogelijkheden van medische apparatuur. De overige vragen zijn niet unaniem beantwoord en behandelen we hieronder.

Resultaten interviews

Beleid, fysieke beveiliging en het afvoeren van medische apparatuur

Beleid

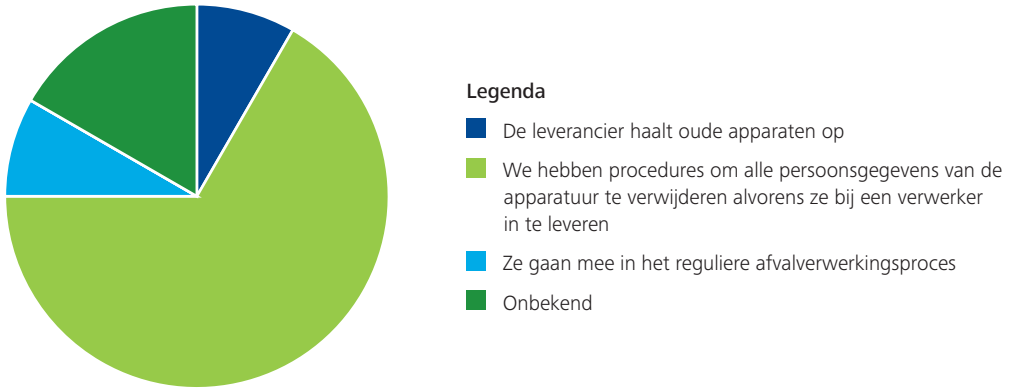
Vier van de geïnterviewde ziekenhuizen gaven aan dat ze expliciet informatiebeveiligingsbeleid voor medische apparatuur voeren. Bij de overige dertien ziekenhuizen bleek dit beleid te ontbreken.



Het is belangrijk om een duidelijk beleid te hebben ten aanzien van de cyber security van medische apparatuur. Het viel ons op dat Medische Technologie en IT soms twee compleet verschillende afdelingen zijn. Hierdoor zijn de verantwoordelijkheden met betrekking tot cyber security van medische apparatuur niet duidelijk. Goed beleid kan hierin duidelijkheid bieden.

Privacy bij afvoeren

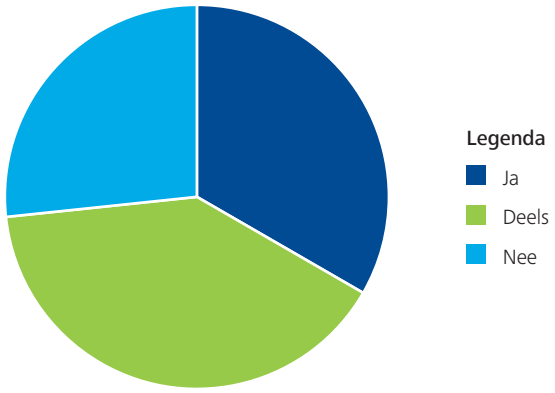
Acht van de geïnterviewde ziekenhuizen gaven aan een procedure te hebben voor het afvoeren van medische apparatuur (als deze verouderd is of niet meer werkt). In één geval wordt de meeste apparatuur opgehaald door de leverancier en bij een ander ziekenhuis wordt de apparatuur ingeleverd bij een professionele afvalverwerker. In twee gevallen wordt de apparatuur vernietigd door een gecertificeerde partij. De ziekenhuizen zonder interne datavernietigingsprocedure doen de aanname dat de leveranciers, gecertificeerde verwerkers zelf op een adequate manier de data verwijderen. Het werd duidelijk dat we deze vraag in onze standaardvragenlijst misten. We hebben de vraag later aan de set vragen toegevoegd waardoor de uitspraak op dit deelgebied minder significant is dan op de andere deelgebieden.



Het risico van het niet of niet goed genoeg verwijderen van data van medische apparatuur is dat privacygevoelige informatie ongewenst op een verkeerde plek kan belanden.

Fysieke beveiliging

Zeven van de geïnterviewde ziekenhuizen gaven aan dat ze grotere medische apparatuur in een afgesloten ruimte bewaren. Voor zes huizen geldt dit deels en in vier gevallen zijn de ruimtes waar de medische apparatuur staan voor al het ziekenhuispersoneel toegankelijk.

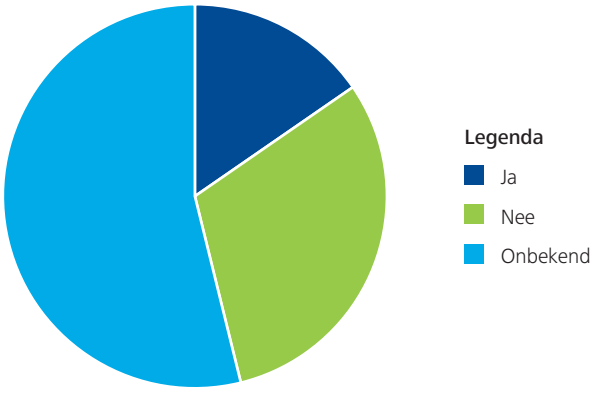


In sommige gevallen is het logisch dat medische apparatuur toegankelijk is voor iedereen die zich in het ziekenhuis bevindt. Een voorbeeld is de hartmonitoringsapparatuur die is gekoppeld aan een patiënt die bezoek kan ontvangen. Het zou echter voorkomen moeten worden dat patiënten, bezoekers en anderen ongeautoriseerde apparatuur (zoals smartphones en USB-sticks) kunnen aansluiten op medische apparatuur. Daarnaast zouden ziekenhuizen moeten bepalen welke ruimtes niet toegankelijk hoeven te zijn voor andere bezoekers, buiten de patiënten om. Zo zou je bij bijvoorbeeld MRI-scanners fysieke toegangsbeveiliging kunnen implementeren.

Data protectie

Communicatie versleuteling

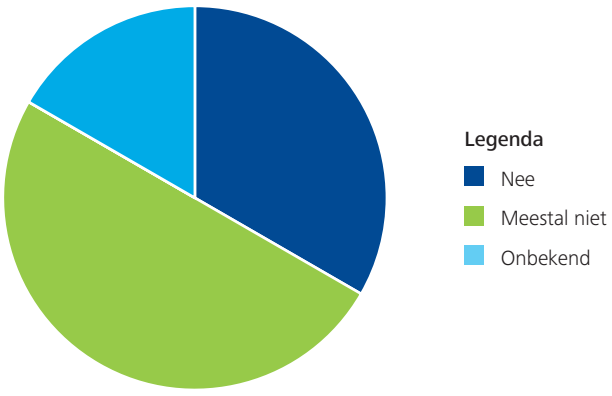
Twee van de geïnterviewde ziekenhuizen gaven aan dat medische apparatuur in het algemeen communiceert over het netwerk met een versleutelde verbinding. Zes ziekenhuizen gaven aan dat dit in het algemeen niet het geval is, zeven ziekenhuizen gaven aan daar geen zicht op te hebben en 2 ziekenhuizen konden de vraag op dat moment niet beantwoorden.



Het risico van het ontbreken van communicatie kan per netwerkarchitectuur verschillen, bijvoorbeeld door netwerksegregatie of network access controls toe te passen. Als deze maatregelen ontbreken, bestaat het risico van netwerkverkeer op een niet-versleuteld netwerk van medische apparatuur waardoor de vertrouwelijkheid van de gegevens niet kan worden geborgd. Daarnaast kan (mits geen additionele maatregelen) de integriteit van de verstuurde informatie in het geding komen. Dit kan uiteindelijk leiden tot een patiëntveiligheidsrisico of inbreuk op de privacy van de patiënt.

Versleuteling USB-stick

Van de geïnterviewde ziekenhuizen gaven acht ziekenhuizen aan dat het meestal niet mogelijk is om gegevens op een USB-stick te versleutelen. Vier ziekenhuizen gaven aan dat dit bij hun organisatie helemaal niet mogelijk is.



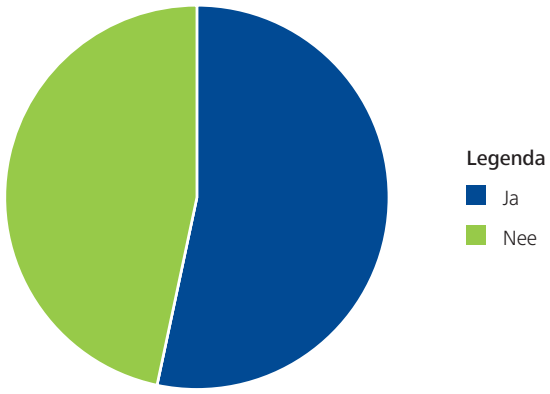
Gegevens kunnen onversleuteld op USB-sticks belanden, waardoor een verhoogd risico bestaat op het lekken van data. Daarnaast is het lastig om de integriteit van de data te garanderen als deze vanaf een USB-stick worden teruggezet op het medische systeem.

Ziekenhuizen kunnen overwegen om de USB-aansluitingen (waar mogelijk) volledig fysiek dicht te maken. Als de aansluiting nodig is voor de werking van het systeem of om de communicatie met andere apparatuur mogelijk te maken, kan worden gewerkt met een losstaand systeem dat een USB-stick eerst op virussen controleert voordat deze wordt gebruikt.

Een veilige oplossing voor het meegeven van afbeeldingen of gegevens aan de patiënt, is deze aan te bieden op een nieuwe USB-stick die het ziekenhuis zelf verstrekt.

Computervirussen

Van de geïnterviewde ziekenhuizen gaven tien aan dat zij weleens te maken hebben gehad met een computervirusbesmetting op hun medische apparatuur. Zeven gaven aan hiervan nooit last te hebben gehad.



Het risico van computervirussen is groot. Aan de ene kant kan de integriteit en de werking van het medische apparaat niet meer worden gegarandeerd als het besmet is met een computervirus. Daarnaast zorgen sommige virussen voor performanceproblemen. Hierdoor komt de beschikbaarheid van het apparaat in gevaar. Als operationele processen binnen het ziekenhuis op dit apparaat steunen, kunnen deze processen en daarmee behandelingen in gevaar komen.

Een virusscanner op een medisch apparaat is niet altijd de oplossing, omdat niet alle apparatuur dit ondersteunt en ziekenhuizen niet altijd bevoegd zijn om software te installeren op door hen aangeschafte apparatuur. Naast netwerksegmentatie zouden Intrusion Detection Systemen (IDS) en Security Information and Event Management (SIEM) systemen een oplossing kunnen bieden. Hiermee kan apparatuur op dezelfde manier worden gebruikt als nu, maar is deze wel weerbaarder tegen besmettingen door malware.

Good practices en tips

Tijdens de interviews zijn we een aantal good practices tegengekomen: beleid, netwerksegregatie, één verantwoordelijke voor ICT en Medische Technologie (MT), Awareness en het inventariseren van apparatuur met bijbehorende risico assessments. Hieronder worden de gevonden good practices beschreven.

Eén verantwoordelijke voor ICT en MT

Eén verantwoordelijke voor ICT en MT zorgt voor een betere en snellere schakeling tussen ICT en MT. Daarnaast zijn de taken en verantwoordelijkheden duidelijk.

Netwerksegregatie

Het administratieve netwerk moet van het medische netwerk gescheiden zijn. Daarnaast kunt u apparaten in subnetwerkgroepen indelen om intern extra beveiliging tegen massabesmettingen te borgen.

Beleid

Een beleid voor de informatiebeveiliging van medische apparatuur zorgt ervoor dat de taken en verantwoordelijkheden duidelijk zijn. Daarnaast moet beleid borgen dat tijdens het inkoopproces de juiste informatie wordt verkregen.

Awareness

Hoe meer medisch technici en IT'ers op de hoogte zijn van de cyberrisico's van netwerk verbonden medische apparatuur, des te eerder worden potentiële dreigingen gesignaleerd en volgt er adequate actie.

Inventariseer apparatuur, connectiviteit en risico's

Het is belangrijk een volledige en up-to-date inventaris van netwerk verbonden medische apparatuur te hebben, inclusief de eigenschappen en het cyberrisicoprofiel van het apparaat.

Conclusie

Toen we begonnen aan dit onderzoek, viel het op dat het onderwerp nieuw was bij ziekenhuizen. Naarmate het interviewtraject vorderde, merkten we dat steeds meer professionals op de hoogte waren van de laatste ontwikkelingen op het gebied van het beveiligen van medische apparatuur.

Het niet gebruiken van medische apparatuur is vooralsnog een groter risico voor de gezondheid van de patiënt dan het gebruiken van kwetsbare medische apparatuur. Maar kwetsbaarheden zijn in sommige gevallen eenvoudig te mitigeren en daarom is het aan te bevelen hiermee aan de slag te gaan.

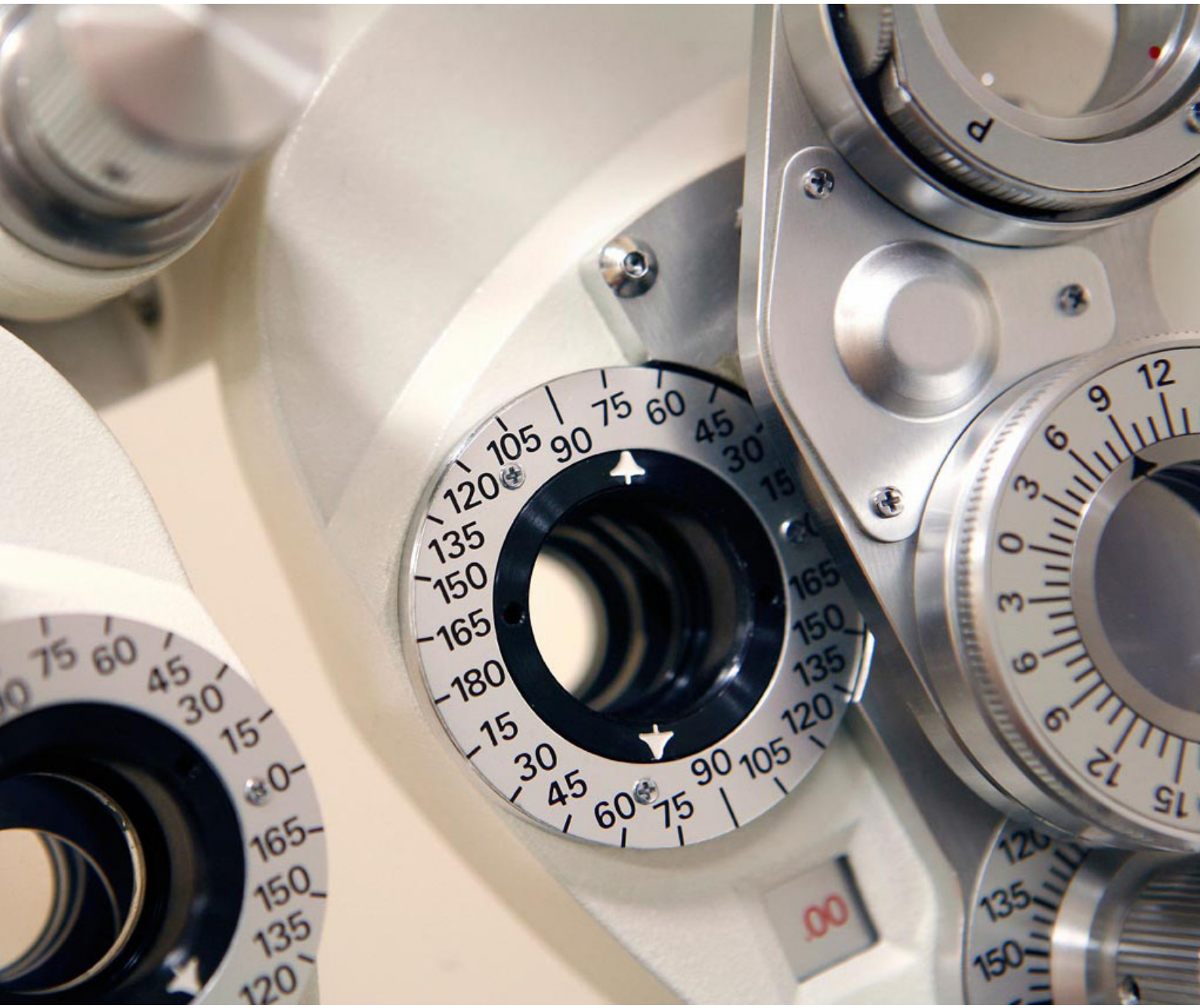
Als algemene conclusie stellen wij dat steeds meer medische apparatuur met een netwerk verbonden is en dat daarmee het cyberrisico van medische apparatuur is toegenomen. Het risico op verstoring door computervirussen werd hier het meeste genoemd. Daarnaast constateerden we de volgende aandachtspunten:

- Bijna een kwart van de ziekenhuizen geeft aan expliciet beleid te hebben voor de informatiebeveiliging van medische apparatuur;
- Meer dan de helft van de ziekenhuizen geeft aan weleens te maken te hebben gehad met een computervirusbesmetting van hun medische apparatuur;
- Minder dan een kwart van de ziekenhuizen geeft aan zeker te weten dat medische apparatuur op een netwerk versleuteling gebruikt;
- Meer dan driekwart van de ziekenhuizen geeft aan het (meestal) niet mogelijk is om gegevens van een medisch apparaat direct versleuteld op een USB-stick op te slaan;
- Iets minder dan driekwart van de ziekenhuizen heeft een adequate procedure om gegevens van medische apparatuur te verwijderen voordat deze wordt afgevoerd.

Het is van groot belang incidenten (zowel als gevolg van gerichte als ongerichte aanvallen) te voorkomen. Dit doen we echter niet door de vele innovatieve oplossingen die Healthcare technologie biedt niet meer te gebruiken. Voor bestaande medische apparatuur kunnen we met netwerksegmentatie, NAC, SOC en SIEM oplossingen de dreigingen mitigeren. Voor nieuwe medische apparatuur nemen we privacy en security vanaf het begin af aan mee. Op deze manier kunnen we op een veilige manier gebruik maken van de vele mogelijkheden die de nieuwe technologie ons te bieden heeft.

Dankwoord

Dit onderzoek had niet kunnen plaatsvinden zonder de hulp van de ziekenhuizen die we mochten interviewen. We willen iedereen hiervoor hartelijk danken. Daarnaast had het rapport niet tot stand kunnen komen zonder de inspanningen van Floris Schoenmakers, Tom-Martijn Roelof, Salo van Berg, Derk Wieringa, Marrit Plat en Marko van Zwam.



Geraadpleegde literatuur

1. United States Government Accountabillity Office, 'Medical Devices – FDA Should Expand Its Consideration of Information Security for Certain Types of Devices', 2012, http://www.gao.gov/assets/650/647767.pdf, geraadpleegd op: 20-01-2015.
2. Nederlandse Zorg Autoriteit, Medische specialistische Zorg – weergave van de markt 2009-2013, 01-12-2013, http://www.nza.nl/104107/105773/742312/Marktscan_medisch_specialistische_zorg_2013.pdf
3. U.S. Department of Health and Human Services/Office of Inspector General, Work plan for Fiscal Year 2014, http://docs.ismgcorp.com/files/external/OIG-Work-Plan-2014.pdf
4. Nationaal Cyber Security Centrum, Cybersecuritybeeld Nederland 4, 10-07-2014, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html
5. Wired/Kim Zetter, It's Insanely Easy to Hack Hospital Equipment, 04-25-2014, http://www.wired.com/2014/04/hospital-equipment-vulnerable/
6. U.S. Food and Drug Administration, Content of Premarket Submission for Management of Cybersecurity in Medical Devices, 02-10-2014, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
7. College Bescherming Persoonsgegevens, Onderzoek naar de beveiliging van het netwerk van het Groene Hart Ziekenhuis, 06-10-2014, https://cbpweb.nl/sites/default/files/atoms/files/rap_2014_netwerkbeveiliging-groene-hart-ziekenhuis.pdf
8. Reuters/Jim Finkle, U.S. Government probes medical devices for possible cyber flaws, 22-10-2014, http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022
9. U.S. Department of Health and Human Serices/Office of Inspector General, Work plan for Fiscal Year 2015, 2015, http://oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf
10. Collge Bescherming Persoonsgegevens, CBP Agenda 2015, 28-01-2015, https://cbpweb.nl/nl/nieuws/cbp-presenteert-toezichtagenda-voor-2015
11. De IT Auditor, 'Beheersen en controleren Cybersecurityrisico's medische apparatuur', 31-03-2015, http://www.deitauditor.nl/business-en-it/cybersecurityrisicos-medische-apparatuur/