Risico's bij het gebruik van Smartapparatuur in het bedrijfsnetwerk

Een onderzoek in de zorgsector

Student

Jeroen Seegers (328928)
Integrale veiligheidskunde
Saxion Deventer

Praktijkbegeleider

De heer Peter Westerveld
Sincerus Consultancy B.V.

Schoolbegeleiders

De heer Wim Smeitink

2e Schoolbegeleider

De heer Christiaan Kiffen

Deventer, 3 juli 2017

Personalia

Student

Jeroen Seegers (328928)
jbseegers@gmail.com
06-24241548

Praktijkbegeleider

De heer Peter Westerveld
peter.westerveld@Sincerus.nl
06-53976659

Schoolbegeleider

De heer Wim Smeitink
d.j.w.smeitink@saxion.nl
06-26887344

2e Schoolbegeleider

dhr. Christiaan Kiffen
c.l.kiffen@saxion.nl
06-22616767

Opdrachtgever

Sincerus Consultancy B.V.
Dr. Van Lookeren Campagneweg 5a
8025BX Zwolle
038-4529829

Onderwijsinstelling en opleiding

Integrale veiligheidskunde
Saxion hogescholen
Handelskade 75
7417 DH Deventer
088-0198888

Datum voltooiing:

3 juli 2017

Voorwoord

Voor u ligt de scriptie ‘Risico’s bij het gebruik van smartapparatuur in het bedrijfsnetwerk’. Het onderzoek naar de risico’s en maatregelen van smartapparatuur is uitgevoerd in de zorgsector. Deze scriptie is geschreven in het kader van mijn opleiding Integrale Veiligheidskunde te Saxion in Deventer, in opdracht van Sincerus Consultancy B.V, nader te noemen Sincerus.

Het onderwerp van mijn onderzoek komt voort uit de wens van mijn stagebedrijf, omdat ze als bedrijf graag over meer kennis willen beschikken en met de laatste ontwikkelingen mee willen gaan met betrekking tot de eventuele risico’s bij het gebruik van smartapparatuur. Dit onderzoek heb ik afgerond door middel van kwalitatief onderzoek. Mijn dank gaat uit naar Peter Westerveld die tijdens mijn afstuderen als praktijkcoach fungeerde. Te allen tijde kon ik bij hem terecht voor vragen of nieuwe inzichten, ik heb zijn begeleiding als zeer prettig ervaren. Ook een woord van dank aan Wim Smeitink en Christiaan Kiffen die zich als begeleiders over mijn onderzoek hebben ontfermd. Hierbij wil ik al mijn begeleiders bedanken voor de prettige samenwerking.

Naast mijn begeleiders wil ik ook de personen die ik heb mogen interviewen voor mijn onderzoek, bedanken. Allereerst wil ik de vier organisaties bedanken, die de tijd hebben genomen om mij te woord te staan over de rol van smartapparatuur in de organisatie. Ik wil Lodewijk Huinink van Medisch Spectrum Twente, Jeroen Geerdink van Ziekenhuisgroep Twente, Niels Drieënhuizen van Lindenhout en Stephan Hazekamp van het St. Jansdal ziekenhuis bedanken voor hun medewerking. Een extra woord van dank aan Gea Wijn, Harald Vranken en Mariëlle Stoellinga voor het delen van hun expertise.

Tot slot wil ik mijn collega’s van Sincerus bedanken voor de fijne tijd die ik daar gehad heb. Ondanks dat ik niet altijd op locatie aanwezig kon zijn, heb ik toch het gevoel gehad dat ik deel uitmaakte van de organisatie. Ik ben goed geholpen en ondersteund door verschillende collega’s tijdens het schrijfproces van mijn onderzoeksrapport.

Veel leesplezier,

Jeroen Seegers

Zwolle, 3 juli 2017

Samenvatting

Door technologische ontwikkelingen is smartapparatuur in opkomst. Werd smartapparatuur voorheen vaak nog gebruikt in de thuissituatie, wordt het nu steeds meer zakelijk toegepast. De gemakken van deze apparaten brengen tegelijkertijd risico's met zich mee.

Het doel van dit onderzoek is, om te kijken of er risico's verbonden zijn aan het gebruik van smartapparatuur in het bedrijfsnetwerk. Daarnaast is onderzocht of het mogelijk is om een adviesproduct te ontwikkelen dat organisaties in de zorgsector kan helpen met het reduceren van beveiligingsrisico's bij smartapparatuur. Hiervoor is de volgende probleemstelling gehanteerd: '*Welke risico's spelen er in de zorgsector bij het gebruik van smartapparatuur in het bedrijfsnetwerk; hoe zijn deze risico's inzichtelijk te maken en welke maatregelen kunnen er getroffen worden om deze risico's te voorkomen?*'

Om een antwoord te vinden op de centrale vraag van dit onderzoek is kwalitatief onderzoek uitgevoerd. Er is een beeld geschetst van de rol van smartapparatuur in de zorgsector met behulp van vier zorgorganisaties. De organisaties bestaan uit drie ziekenhuizen en een individuele zorginstelling. De risico's en maatregelen zijn onderzocht aan de hand van interviews met experts en door het maken van een risicoanalyse. De vier organisaties die zijn onderzocht in de zorgsector maken allemaal gebruik van smartapparatuur. Smart-tv's en smartwatches komen in alle vier de organisaties voor, maar smart health komt alleen voor in de ziekenhuizen. In totaal zijn er zestien verschillende soorten smartapparatuur genoemd door de organisaties. Alle onderzochte organisaties voeren een beleid omtrent smartapparatuur. De organisaties voeren allen een risicoanalyse uit als er nieuwe apparatuur wordt aangeschaft. Daarnaast worden er weinig tot geen standaardwachtwoorden veranderd van de smartapparatuur.

Doordat smartapparatuur in de zorgsector een rol speelt, is het essentieel om te kijken welke risico's eraan kleven wanneer deze wordt gebruikt in een bedrijfsnetwerk. Er zijn tal van risico's te noemen. Volgens experts zit de beveiliging van de smartapparatuur nog op een laag niveau. Producenten nemen dit niet mee in de design-fase. Het is soms niet mogelijk om het product te updaten of om het standaardwachtwoord te veranderen. Dit komt doordat de producent een korte '*time-to-market*' wil. Een ander risico is dat de standaardwachtwoorden makkelijk te raden zijn wanneer deze niet worden veranderd. De uitdaging van smartapparatuur is de beveiliging. Het is belangrijk dat de smartapparatuur juist wordt gebruikt, omdat daar ook risico's in schuilen. Medewerkers willen zo snel mogelijk bij patiëntgegevens, zijn niet bereid om veel wachtwoorden in te voeren, zijn minder bereid om regels na te leven en omzeilen security uit gemak. Er wordt ook vaak gedacht dat andere organisaties sneller worden getroffen. De impact van deze risico's zijn groot. Doordat patiëntgegevens kunnen worden aangepast, is er de mogelijkheid dat er verkeerde zorg wordt geleverd. Dit kan fatale gevolgen hebben.

De belangrijkste maatregelen die getroffen moeten worden volgens de experts zijn: het uitvoeren van risicoanalyses, het maken van beheersplannen, het geven van awareness-trainingen met co-creatie en iemand verantwoordelijk stellen voor de security in de organisatie. De belangrijkste maatregelen die uit de gemaakte risicoanalyse komen zijn: het aanschaffen van veilige producten, het kopen van smartapparatuur dat al langer op de markt is, het gebruiken van smartapparatuur alleen wanneer het daadwerkelijk nodig is, het zoeken naar standaardisatie, het updaten van smartapparatuur, het veranderen van standaardwachtwoorden, het aansluiten van smartapparatuur op het gastnetwerk, het voeren van beleid dat aangeeft welke medewerker waar bij kan, het geven van vertrouwen aan gebruikers en het lezen van privacy voorwaarden. De risico's en maatregelen worden verwerkt in een checklist. Uit een gesprek met de opdrachtgever Sincerus is naar voren gekomen dat het een adviesproduct betreft, die wordt gebruikt in de voorfase van het advies. Met dit product is het wenselijk om potentiële klanten binnen te halen. Het is de wens van Sincerus dat er in het product schematisch wordt weergegeven wat een organisatie in de zorgsector kan doen om zich te wapenen tegen de risico's van smartapparatuur.

Inhoudsopgave

Begrippenlijst

Botnet: dit is een netwerk van geïnfecteerde computers waar een cybercrimineel op afstand gebruik van maakt, voor eigen doeleinden en gewin. De cybercrimineel maakt hierbij gebruik van de rekencapaciteit en netwerkfunctionaliteit van de bots over de hele wereld. Het is een infrastructuur waarbij de identiteit van de cybercrimineel niet bekend wordt gemaakt. Via deze botnets wordt onder andere malware, spam, DDoS-aanvallen en keylogging verspreid (Nationaal Cyber Security Centrum, 2012).

Cybercrime in enge zin: strafbare gedragingen die niet zonder tussenkomst of gebruik van ICT gepleegd kunnen worden. De doelwitten van deze actie zijn: apparatuur, hardware of software. ICT-middelen moeten het doelwit zijn en de daad moet uitgevoerd worden door misbruik te maken van ICT-voorzieningen (Nationaal Cyber Security Centrum, 2012).

Cybercrime in ruime zin: strafbare gedragingen die met behulp van of via ICT worden uitgevoerd. Traditionele criminaliteit wordt ondersteund door ICT-middelen of digitale technieken (Nationaal Cyber Security Centrum, 2012).

Cybersecurity: het vrij zijn van gevaar of schade, veroorzaakt door verstoring van ICT, uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (Nationaal Cyber Security Centrum, 2016).

DDoS-aanval: een Distributed Denial of Service-aanval wordt uitgevoerd vanaf een groot aantal IP-adressen tegelijk. Bij deze aanval wordt geprobeerd een computer, een systeem of telecommunicatienetwerk te overbelasten zodat deze wordt uitgeschakeld en niet meer beschikbaar is voor gebruikers. Deze aanval wordt uitgevoerd door grote hoeveelheden data te versturen in de vorm van een e-mail of door ander netwerkverkeer (Nationaal Cyber Security Centrum, 2012).

Domotica: via domotica worden verschillende apparaten aan elkaar gekoppeld door middel van een protocol, zodat processen in een woning geautomatiseerd kunnen worden. Domotica kan er bijvoorbeeld voor zorgen dat wanneer er een raam wordt geopend, de verwarming automatisch omlaag gaat (Smart-Homes, 2016).

Internet of Things: alle apparaten die in verbinding staan met het internet zoals computers, tablets en servers. Naast deze apparaten vallen ook slimme apparaten zonder scherm, die in verbinding staan met internet, onder deze categorie. Denk hierbij aan koelkasten, verwarmingssystemen en auto's. Deze apparaten hebben allemaal een eigen IP-adres en staan in verbinding met elkaar door te communiceren. Veel van deze apparaten zijn te bedienen met een app op de mobiele telefoon (Domotica, 2017).

Malware: dit is een verzamelnaam voor software met kwade bedoelingen, zoals virussen (Nationaal Cyber Security Centrum, 2012).

Ransomware: bij deze vorm van malware krijgt een slachtoffer een bericht, waarin een betaling wordt gevraagd om versleutelde software te kunnen openen. Door het slachtoffer naar een website te lokken installeert de hacker, buiten het weten van de gebruiker om, een programma die een computerbestand versleutelt. Wanneer de betaling voltooid is, worden de bestanden weer vrijgegeven (Nationaal Cyber Security Centrum, 2012).

Smartapparatuur: dit is een verzamelnaam voor elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kunnen zijn op een intern netwerk en met elkaar kunnen communiceren.

1. Inleiding

1.1 Aanleiding

Op 21 oktober 2016 hebben hackers aan de oostkust van de Verenigde Staten, een 'Distributed Denial of Service-aanval' uitgevoerd op een DNS-provider, waardoor de sites Pinterest, Twitter, Reddit, Github, Etsy, Tumblr, Spotify, PayPal, Comcast, Verizon en het Playstation Netwerk niet meer goed functioneerden. Deze DDoS-aanval is uitgevoerd met behulp van smartapparatuur, zoals printers en beveiligingscamera's. Bij een DDoS-aanval stuurt een hacker een enorme hoeveelheid data, zodat een computer of website overbelast raakt (Van Beurden, 2014). Er werd via tientallen miljoenen IP-adressen een aanval uitgevoerd, door tegelijkertijd data te versturen vanaf meerdere apparaten. Doordat de aanval was gericht op een Dyn, een soort telefoonboek voor het internet, konden er meerdere websites tegelijkertijd niet meer goed werken (Domotica, 2016).
Veel connected-devices die in deze aanval zijn gebruikt, zijn van Chinese afkomst en konden niet goed beveiligd worden. Dit kwam doordat er standaardwachtwoorden op de apparaten zaten, die niet gewijzigd konden worden. Om meer data te sturen dan voorheen met alleen computers mogelijk was, werden deze smartapparatuur vervolgens gebruikt als een botnet (Cobb, 2016). Door veel apparaten op de markt te brengen die niet goed beveiligd zijn, is de kans groter dat het dagelijks leven en de economie schade kan oplopen. Als de online verkoop stil komt te liggen en er geëvalueerd moet worden over hoe er met dit soort aanvallen moet worden omgegaan, kunnen bedrijven grote financiële schade leiden.

1.1.1 Inspelen op ontwikkelingen

Smartapparatuur kan in de categorie 'Internet of Things' worden geschaard. Dit is de verzamelnaam van alle connected devices zoals computers, smartphones, tablets en apparaten zonder scherm. De apparaten staan met elkaar in verbinding via IP-adressen en worden vaak bediend door middel van een app op de smartphone (Domotica, 2017). Doordat deze apparaten sterk in opkomst zijn, zijn ze gelijk ook een doelwit geworden voor kwaadwillende personen. Hierdoor is er sprake van toenemende impact van beveiligingsincidenten. De voor consumenten gemaakte smartapparatuur zal steeds meer in bedrijfsnetwerken worden opgenomen (Knieriem, 2016). Sincerus wil graag inspelen op deze huidige ontwikkelingen in de wereld van informatiebeveiliging, door te onderzoeken op welke manier het mogelijk is om advies te geven aan organisaties over de mogelijke risico's die spelen bij het gebruik van smartapparatuur in het bedrijfsnetwerk (Sincerus, 2017). Tot op heden wordt er door Sincerus nog geen advies gegeven over dit onderwerp. Om te voorkomen dat organisaties geen omzet mislopen, is het voor organisaties belangrijk dat het bedrijfsproces niet stilvalt.

1.2 Doelstelling

Het doel van dit onderzoek is het ontwikkelen van een beleidsproduct, waarmee Sincerus advies kan geven aan nieuwe en bestaande klanten. Dit advies heeft betrekking op primaire bedrijfsprocessen die risico lopen bij het gebruik van smartapparatuur in het bedrijfsnetwerk. Nadat het onderzoek is uitgevoerd, kan er aan Sincerus advies worden gegeven over hoe een eventueel adviesproduct eruit moet zien. Als Sincerus organisaties kan adviseren over deze risico's, kan Sincerus meer opdrachten binnenhalen en kan Sincerus ervoor zorgen dat bedrijfsprocessen niet worden onderbroken. Dit is een zowel een economisch als een maatschappelijk doel, doordat de Nederlandse economie door dit advies zo min mogelijk schade oploopt.

1.3 Probleemstelling

Om de doelstellingen te behalen, moet er onderzocht worden welke risico's er spelen en welke maatregelen er moeten worden getroffen bij het gebruik van smartapparatuur in een bedrijfsnetwerk. Daarnaast moet er onderzocht worden hoe deze inzichtelijk kunnen worden gemaakt. Om dit te onderzoeken is de volgende probleemstelling opgesteld:

'*Welke risico's spelen er in de zorgsector bij het gebruik van smartapparatuur in het bedrijfsnetwerk, hoe zijn deze eventuele risico's inzichtelijk te maken en welke maatregelen kunnen er getroffen worden om eventuele risico's te voorkomen?*'

1.3.1 Onderzoeksvragen

Om de probleemstelling te kunnen beantwoorden zijn de volgende onderzoeksvragen opgesteld:

- In welke mate speelt smartapparatuur een rol in de zorgsector?
- Welke risico's zijn er aanwezig bij het gebruik van smartapparatuur in het bedrijfsnetwerk en in welke mate zijn organisaties zich bewust van deze risico's?
- Waar moet een adviesproduct volgens Sincerus aan voldoen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector?

1.4 Belanghebbenden

Sincerus Consultancy B.V.

De belangrijkste belanghebbende is Sincerus. Sincerus is een onafhankelijk bedrijf dat adviezen geeft op het gebied van informatiebeveiliging in de zakelijke wereld. Door middel van aandacht voor beschikbaarheid van data, betrouwbaarheid van data, contingency en de menselijke factor helpt Sincerus organisaties bij het implementeren en borgen van het gewenste niveau van informatiebeveiliging (Sincerus, 2017). Om te zorgen voor het gewenste niveau van informatiebeveiliging is het van belang om trainingen, advies en begeleiding te geven. Het is ook belangrijk om risicoanalyses uit te voeren, om te kijken aan welke risico's en dreigingen een bedrijfsproces wordt blootgesteld. Sincerus heeft er belang bij, omdat ze de klanten een breder niveau van informatiebeveiliging kunnen bieden. Naar aanleiding van dit onderzoek kunnen er eventueel meer opdrachten worden binnengehaald.

Klanten

De klanten van Sincerus hebben belang bij dit onderzoek. Als Sincerus advies kan geven over mogelijke risico's bij het gebruik van smartapparatuur in het bedrijfsnetwerk, is dat voordelig voor de klanten die het advies ontvangen. Zo kunnen deze organisaties zorgen dat er minder risico wordt gelopen bij het gebruik van deze apparaten. Op deze manier is er een kleinere kans op het stilvallen van het vitale productieproces, waarbij er mogelijk geld verloren kan gaan. Vooral de klanten uit de zorgsector hebben hier belang bij.

Concurrenten

In het eerste kwartaal van 2017 zijn er naar de standaardbedrijfsindeling van het SBI2008, 16.635 adviesbureaus op het gebied van Informatietechnologie. Deze klasse omvat:

- consultancy;
- advisering op het gebied van hard- en software;
- ontwikkelen, samenstellen en programmeren van gebruiksklare systemen;
- integratie van hard- en software en communicatietechnologie (CBS Statline, 2017).

Adviserende Informatiebeveiligingsbedrijven vallen ook onder deze categorie.

Concurrenten die nog niet bezig zijn met het advies geven over het gebruik van smartapparatuur in het bedrijfsnetwerk, zullen achter lopen. Potentiële klanten zullen sneller met Sincerus in zee gaan, omdat

medewerkers van Sincerus in staat zijn om een breder advies te geven. Dit is helemaal van toepassing wanneer een klant specifiek het gebruik van smartapparatuur wil verbeteren.

Kwaadwillenden

Er zijn een hoop kwaadwillenden waarvoor dit onderzoek van belang is. Als Sincerus meer klanten kan helpen met het veilig maken van smartapparatuur, dan kunnen kwaadwillenden minder bereiken. Deze kwaadwillenden hebben allemaal verschillende doelen en zijn op te splitsen in de volgende categorieën: beroepscriminelen, statelijke actoren, terroristen, cybervandalen en scriptkiddies, hacktivisten, interne actoren en private organisaties (Nationaal Cyber Security Centrum, 2016). Volgens het Nationaal Cyber Security Centrum zijn dit de beweegredenen van deze kwaadwillenden:

- **Beroepscriminelen:** deze categorie kwaadwillenden vormen een dreiging voor de Nederlandse digitale veiligheid. Door middel van digitale aanvallen en afpersingen willen deze criminelen geld verdienen. Particulieren, organisaties en de Nederlandse overheid zijn doelwitten.
- **Statelijke actoren:** Nederlandse overheden, de economie en de nationale veiligheid worden bedreigd door statelijke actoren. Deze actoren hebben als doel om de geopolitieke machtspositie te verbeteren door te bespioneren. Deze digitale aanvallen zijn aantrekkelijk vanwege de lage kosten, beperkte afbreukrisico's en de hoeveelheid informatie die wordt opgebracht.
- **Terroristen:** door het uitvoeren van kleinschalige digitale aanvallen, wordt er geprobeerd om maatschappelijke onrust te creëren. Kennis en vaardigheden zijn niet essentieel bij het uitvoeren van deze aanvallen. Een ander doel is om angst te creëren, of politieke besluitvorming te beïnvloeden.
- **Cybervandalen en scriptkiddies:** deze groepen plegen steeds meer digitale aanvallen, omdat er een groeiende beschikbaarheid is van laagdrempelige hulpmiddelen. Het doel van deze aanvallen is: de uitdaging, het laten zien wat de eigen capaciteiten zijn of gewoon uit baldadigheid. Deze groep bestaat over het algemeen uit minderjarigen, met een variërend kennisniveau.
- **Hacktivisten:** Dit is een groep kwaadwillenden met verschillende motieven en capaciteiten om een aanval uit te voeren. De motieven zijn altijd vanuit een eigen ideologie. Tijdens internationale conflicten en aanslagen zijn hacktivisten actiever dan normaal. De digitale aanvallen zijn gericht op overheidsdoelen, de media en organisaties.
- **Interne actoren:** deze actoren kunnen intern veel schade aanrichten. Dit kan komen doordat de medewerkers onbewuste acties uitvoeren, onzorgvuldig zijn of bewust kwaadwillend zijn. Kwaadwillende medewerkers manipuleren bewust gegevens of systemen vanuit financiële, politieke of persoonlijke motieven.
- **Private organisaties:** de doelen die private organisaties hebben bij een aanval op andere organisaties kunnen zijn: de vertrouwelijkheid van systemen aantasten om geld te verdienen, het verbeteren van de concurrentiepositie, het verzamelen van data om deze te gebruiken en het verzamelen van data om deze te verkopen aan derden.

2. Theoretisch kader

In dit hoofdstuk wordt duidelijkheid verschaft over het kennisgebied, de centrale begrippen en de thematiek. Allereerst worden de kaders van dit onderzoek duidelijk door het toelichten van cybersecurity in Nederland, domotica, Internet of Things en smartapparatuur. Vervolgens worden relevante wetten en ISO-Normen weergegeven. Tot slot wordt de methode van de risicoanalyse en de invulling van Business continuity management in dit onderzoek toegelicht.

2.1 Cybersecurity Nederland

Dit onderzoek is te plaatsen in het vakgebied cybersecurity. Cybersecurity is volgens het Cybersecuritybeeld 2016: 'Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (Nationaal Cyber Security Centrum, 2016).' De volgende ontwikkelingen in de cybersecurity zijn relevant om te benoemen, omdat deze invloed konden hebben op het onderzoek:

DDoS-aanvallen

Er zijn in 2016 veel DDoS-aanvallen waargenomen. Degenen die verantwoordelijk zijn voor deze aanvallen zijn voornamelijk: criminelen, cybervandalen, hacktivisten en scriptkiddies. Niet alleen het platleggen van websites en systemen is een doel, maar het is ook steeds meer een doel om via deze weg slachtoffers af te persen. Maatregelen tegen deze aanvallen zijn vaak effectief, maar vereisen wel een investering. Er wordt nu door private partijen gewerkt om DDoS-bescherming makkelijker en goedkoper te maken (Nationaal Cyber Security Centrum, 2016).

Ransomware

Ransomware wordt steeds meer algemeen bekend en als maar geavanceerder. De malware zelf is verfijnder geworden. Voorheen werden er alleen nog maar bestanden van lokale schijven versleuteld. Nu worden er ook databases, bestanden op netwerkschijven en back-ups gepakt. Voorheen werd er dezelfde prijs betaald per besmetting, maar nu wordt de prijs betaald per getroffen organisatie (Nationaal Cyber Security Centrum, 2016).

Beroepscriminelen

Beroepscriminelen, die bezig zijn met hacken, hebben zich ontwikkeld in de afgelopen jaren. De criminelen zijn veel geavanceerder geworden en voeren nu langdurige campagnes uit, die veel hoogwaardiger zijn dan voorheen. Er worden hoge investeringen gedaan waaruit blijkt dat er een hoge organisatiegraad is. 'Spearphising' wordt ook steeds verfijnder en geloofwaardiger, wat betekent dat het lastiger te bestrijden is met beveiligingsbewustzijn (Nationaal Cyber Security Centrum, 2016).

2.2 Domotica en Internet of Things

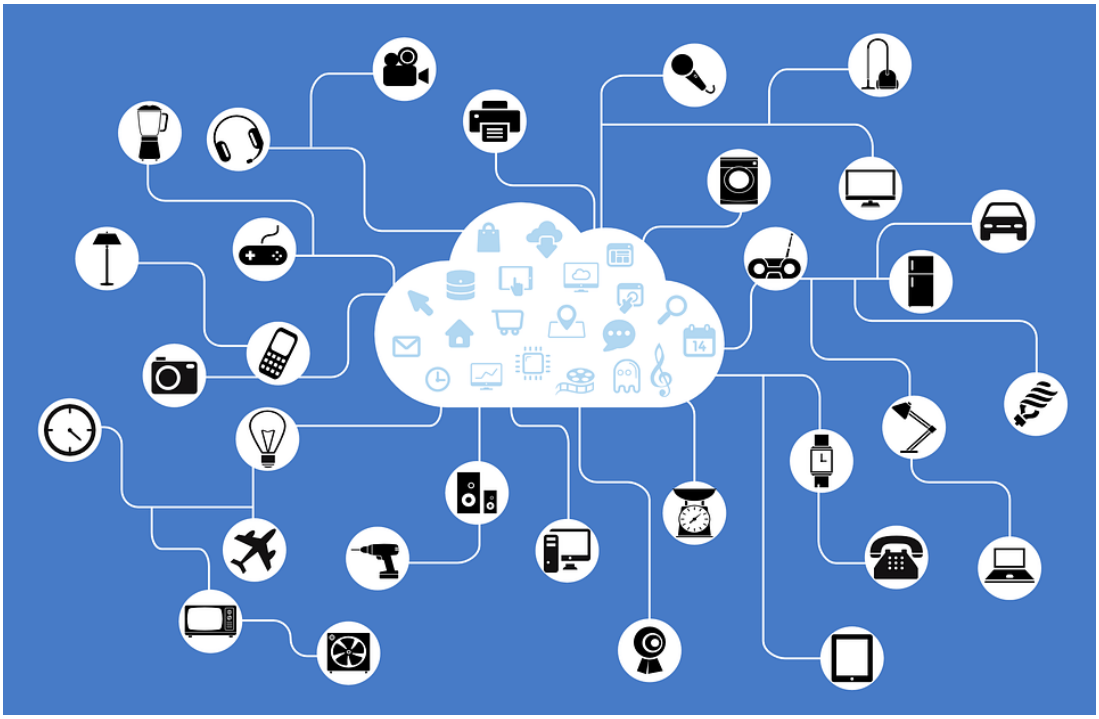
In het onderzoek wordt gekeken naar zogeheten smartapparatuur. Voordat het onderzoek kon worden gedaan, was het eerst van belang om dit begrip af te bakenen. Er zijn namelijk verschillende termen die iets kunnen zeggen over deze apparaten. Zo zijn er de termen Internet of Things en domotica' Deze begrippen lijken op elkaar, maar er zijn toch verschillen. De begrippen worden nu nog vaak verweven (Domotica, 2017). Volgens de website Domotica.nl zijn Internet of Things alle apparaten die in verbinding staan met het internet zoals computers, tablets en servers. Naast deze apparaten vallen ook slimme apparaten zonder scherm, die in verbinding staan met internet, behoren tot deze categorie. Denk hierbij aan koelkasten, verwarmingssystemen en auto's. Deze apparaten hebben allemaal een eigen IP-adres en staan in verbinding met elkaar door te communiceren. Veel van deze apparaten zijn te bedienen met een app op de smartphone. Domotica is slechts een klein onderdeel van het Internet of Things en is een

samentrekking van de Latijnse woorden domus (woning) en telematica (Smart-Homes, 2016). Volgens het kenniscentrum voor Domotica en Slim Wonen koppelt domotica apparaten aan elkaar via een protocol zodat processen in een woning geautomatiseerd worden. Domotica kan er bijvoorbeeld voor zorgen dat wanneer er een raam wordt geopend, de verwarming automatisch omlaag gaat. Het grote verschil met Internet of Things, is dat domotica ook werkt zonder een internetverbinding (Hager, 2017). Internet of Things is namelijk wel afhankelijk van internetverbindingen. Internet of Things bestaat dus voornamelijk uit slimme apparaten. In de toekomst zullen er alledaagse objecten worden ontwikkeld die onder deze categorie vallen, zoals kleding (Alles Verbonden, 2017). In dit onderzoek gaat het over de apparaten en objecten die in verbinding staan met het internet. Het gaat hier niet over computers, mobiele telefoons of tablets. Er kan dus niet enkel over domotica of Internet of Things worden gesproken, omdat deze begrippen heel breed zijn. Er wordt daarom gekozen voor het begrip smartapparatuur.

2.3 Smartapparatuur

Smartapparaten zijn elektronische apparaten die verbinding kunnen maken, communiceren met de gebruiker en kunnen communiceren met andere smartapparatuur. Deze smartapparaten zijn bedoeld om de mens te ondersteunen in zijn functioneren (Lectoraat Smart Devices, 2017). Binnen het lectoraat Smart Devices van de hogeschool Zuyd wordt de volgende definitie gehanteerd: ‘Smart device is een product dat met zo min mogelijk signaalmetingen en maximale interpretatie een mens ondersteunt in zijn functioneren.’ Volgens de Eastern Connecticut State University moet smartapparatuur ook altijd in verbinding staan met wifi, 3G, 4G of andere netwerken (Eastern Connecticut State University, 2014).

In dit onderzoek wordt van deze definities afgeweken, omdat het in dit onderzoek alleen gaat over ‘nieuwe’ smartapparatuur. Het gaat hier niet over computers, mobiele telefoons of tablets. Het is daarom goed om een eigen definitie te hanteren die gebaseerd is op bestaande definities. Deze definitie luidt als volgt: ‘Smartapparaten zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kunnen zijn op een intern netwerk en met elkaar kunnen communiceren.’ Er is smartapparatuur in overvloed en de mogelijkheden zijn eindeloos. In afbeelding 1 is te zien hoe veelzijdig de apparaten zijn en hoe deze met elkaar in verbinding staan.



Afbeelding 1 Slimme apparaten staan in verbinding met elkaar. (Alles Verbonden, 2017)

Volgens het onafhankelijke marktonderzoeksbureau GFK zijn er verschillende categorieën smartapparatuur te onderscheiden voor thuisgebruik (GFK, 2016). Deze categorieën zijn:

- Smart Domestic Appliances (huishoudelijke apparaten)
- Smart Entertainment
- Smart Energy
- Smart Lightning
- Smart Motorisation
- Smart Security
- Smart Communication
- Smart Health

Deze categorieën smartapparatuur komen steeds meer voor in het bedrijfsleven. In de toekomst bestaat er een mogelijkheid dat er meer categorieën kunnen ontstaan. Producten uit deze categorieën, die in bedrijven voor kunnen komen, zijn volgens de website 'Alles Verbonden' (Alles Verbonden, 2017) onder andere:

- Slimme Thermostaat
- Slimme verlichting
- Slimme lampen
- Slimme koelkast
- Wifi Koelkast
- Slimme wasmachine
- Slimme droger
- Slimme stofzuiger
- Robot stofzuiger
- Slimme deurbel
- Smart-tv
- Slimme sloten
- Smart alarm
- Slimme tas
- Smartwatch
- Slimme stekker
- Slimme horloges
- Slimme koffiemachine
- Slimme meter
- IoT-sensoren

2.4 Risico's

Er zijn verschillende manieren om naar risico's te kijken. De manier waarop je naar risico's kijkt, bepaalt hoe je er mee om gaat (Van Alphen & Verhage, 2011). Volgens Van Alphen en Verhage kun je risico's bekijken op de volgende manieren:

- ze horen bij het leven;
- het wordt bepaald door medewerkers;
- het leven wordt beheerst door wetten en regels;
- het kan worden gezien als kansbenadering;
- een wisselwerking tussen technische-, organisatorische- en gedragsfactoren
- het beheersen van potentiële risico's door het aanbrengen van barrières.

Daarnaast kan er nog worden gekeken naar de interactie tussen mens, risicobron en omgeving, het systeem van een bedrijf of de human factors. Alphen en Verhage zeggen dat een risico de kans is dat een incident plaatsvindt, vermenigvuldigt met het effect van dit incident. Om te bepalen wat de omvang van het risico is, kon de ranking methode van Kinney en Wiruth worden gebruikt (Van Alphen & Verhage, 2011). In dit onderzoek is deze methode niet toegepast. Deze methode laat alleen zien of een risico aandacht vereist of dat het slechts een aanvaardbaar risico is. In deze methode komt niet naar voren hoe deze risico's aangepakt kunnen worden. Het is daarom beter om een allesomvattende methode te gebruiken.

2.5 Koepelmethodiek

Om de risico's van smartapparatuur in kaart te brengen, is er gebruik gemaakt van de koepelmethodiek voor de risicoanalist uit het 'Handboek Risicoanalysemethodieken' (Dijkzeul, Mil, & Pennen, 2006). De koepelmethodiek geeft een duidelijk beeld van verschillende stappen die in een risicoanalyse kunnen worden onderscheiden. Deze risicoanalyse is toegepast op bedrijfsprocessen van de zorgorganisaties. Er moet rekening worden gehouden dat dit slechts één manier is om het te doen. Volgens Dijkzeul, Mil & Pennen worden hierbij vier fasen onderscheiden. Bij elke fase worden er een paar vragen gesteld die ondersteund kunnen worden met modellen. De methodiek is letterlijk overgenomen uit het handboek van Dijkzeul, Mil & Pennen.

1. Analyse van vitale belangen en systemen: modellen en methodieken waarmee vitale belangen en systemen in kaart kunnen worden gebracht. Daarbij is er aandacht voor de producten en diensten waarop deze belangen betrekking hebben en de processen en knooppunten die relevant zijn bij de voortbrenging van die producten en diensten. Hierbij is er ook aandacht voor de afhankelijkheid van andere vitale producten en systemen.

Vragen over vitale belangen en systemen

- Wat zijn vitale producten en diensten?
- Welke situaties proberen we te voorkomen?
- Hoe zien de sector en de relevante omgeving eruit?
- Wat zijn de relevante processen en systemen bij de totstandkoming van die producten en diensten?
- Wat zijn de relevante (geografische, fysieke of virtuele) knooppunten bij de totstandkoming van die producten en diensten?
- Welke partijen zijn verantwoordelijk voor deze processen, systemen en knooppunten?
- Welke lagen zijn er in de bedrijfskolom te onderscheiden?
- Welke externe ontwikkelingen leiden mogelijk tot kwetsbaarheden?
- Wat zijn onderliggende afhankelijkheden tussen de vitale producten en diensten?

2. Identificatie van dreigingen: modellen en methodieken waarmee dreigingen kunnen worden geïdentificeerd.

Vragen over identificatie van dreigingen

- Welke (typen) dreigingen kunnen zich (in de toekomst) voordoen?
- Wat is de weerstand van de bestaande systemen?
- Wat zijn de (typen) kwetsbaarheden in de huidige situatie?
- Hoe kan (de aard van en de kans op) bewust menselijk handelen in kaart worden gebracht?
- In welke beheersgebieden doen de dreigingen zich voor?
- Hoe kunnen die dreigingen ten opzichte van elkaar worden beoordeeld en geprioriteerd?

3. Beoordelen en prioriteren van impact: modellen en methodieken waarmee risico's en effecten kunnen worden beoordeeld en geprioriteerd. Daarbij gaat het onder meer om verschillende kans-effect-analyses en analyses van kwetsbaarheid en weerstand.

Vragen over beoordeling en prioritering van impact

- Hoe is de impact in kaart te brengen?
- Wat voor (typen) effecten kunnen zich voordoen?
- Wat zijn de meest relevante kans-effect-combinaties?
- In welk beheergebied doet het effect zich voor?
- Hoe lang duurt het voordat de schade optreedt en wat is de hersteltijd?

4. Formulering, beoordeling en implementatie van maatregelen: modellen en methodieken waarmee bestaande maatregelen in kaart kunnen worden gebracht, nieuwe maatregelen kunnen worden geformuleerd en beoordeeld en de implementatie ervan kan worden gemonitord. Daarbij is er ook aandacht voor draagvlak en de kosten en baten van maatregelen.

Vragen over de formulering, beoordeling en implementatie van maatregelen

- Welke typen maatregelen zijn te onderscheiden?
- Welke bestaande maatregelen zijn al genomen?
- Welke aanvullende maatregelen zijn benodigd?
- In welk krachtenveld moeten maatregelen geïmplementeerd worden?
- Hoe hoog zijn de kosten en baten van verschillende maatregelen?
- Welke partijen zijn verantwoordelijk voor de maatregelen?
- Welke maatregelen kunnen op draagvlak rekenen en welke niet?
- Wat is de afdwingbaarheid van maatregelen?
- Hoe kunnen maatregelen vergeleken worden?
- Via welke aanpak is de implementatie van maatregelen te monitoren?
- Hoe robuust zijn maatregelen in de tijd?
- In hoeverre past een maatregel bij de kenmerken van de markt?

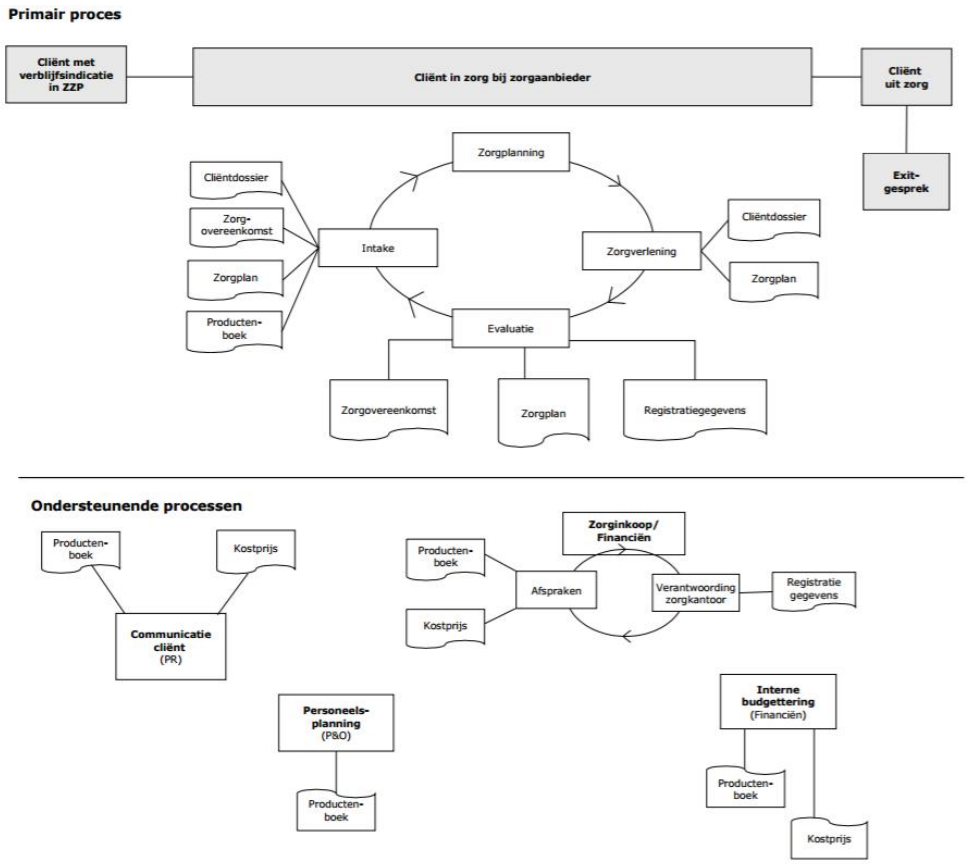
2.6 Business Continuity Management

Bij het gebruik van smartapparatuur spelen risico's, die in kaart zijn gebracht door het toepassen van de koepelmethodiek. Deze risico's kunnen invloed hebben op bedrijfsprocessen van een organisatie en kunnen discontinuïteit veroorzaken. De bedrijfscontinuïteit is essentieel voor organisaties en dat geldt ook voor organisaties in de zorgsector. Wanneer vitale processen uitvallen, kan dit fatale gevolgen hebben. Theorieën van Business Continuity Management kunnen daarom ondersteunend zijn in dit onderzoek. Business Continuity Management is het proces waarbij potentiële dreigingen voor bedrijfsprocessen worden geïdentificeerd en waarbij kaders gesteld worden voor het creëren van organisatorische veerkracht. Hierbij worden de belangen van stakeholders, de reputatie, het merk en waarde creërende activiteiten gewaarborgd (Business Continuity Institute, 2013). Er zijn veel factoren van invloed op de bedrijfscontinuïteit van een organisatie. Volgens de ISO 22301 norm (CEN, 2014) zijn er meerdere factoren van belang bij het organiseren van een goed Business Continuity Managementsysteem. Het is belangrijk om als organisatie te weten wat de activiteiten, functies, diensten, en logistieke ketens zijn. Het is ook belangrijk om te weten wie de belanghebbenden zijn en wat de mogelijke gevolgen van een verstorend incident zijn. Daarnaast zijn interne en externe factoren van belang om aan te kunnen tonen welke kunnen leiden tot een risico. ICT is een onmisbaar instrument voor de bedrijfscontinuïteit van bijvoorbeeld een ziekenhuis (Rahusen & Reemer, 2010).

2.6.1 Bedrijfsprocessen

Om te onderzoeken waar eventuele risico's zich binnen de organisaties kunnen voordoen, was het van belang om de primaire en secundaire bedrijfsprocessen in kaart te brengen. Primaire processen zijn alle activiteiten die rechtstreeks een bijdrage leveren aan het tot stand komen van een product of dienst, zoals produceren en verkopen. Secundaire processen zijn processen die worden uitgevoerd om productiefactoren in stand te houden, zoals personeel en informatiesystemen (Van Dam & Marcus, 2015). De processen in de zorg zijn weergegeven in de volgende paragrafen.

Processen in de zorg



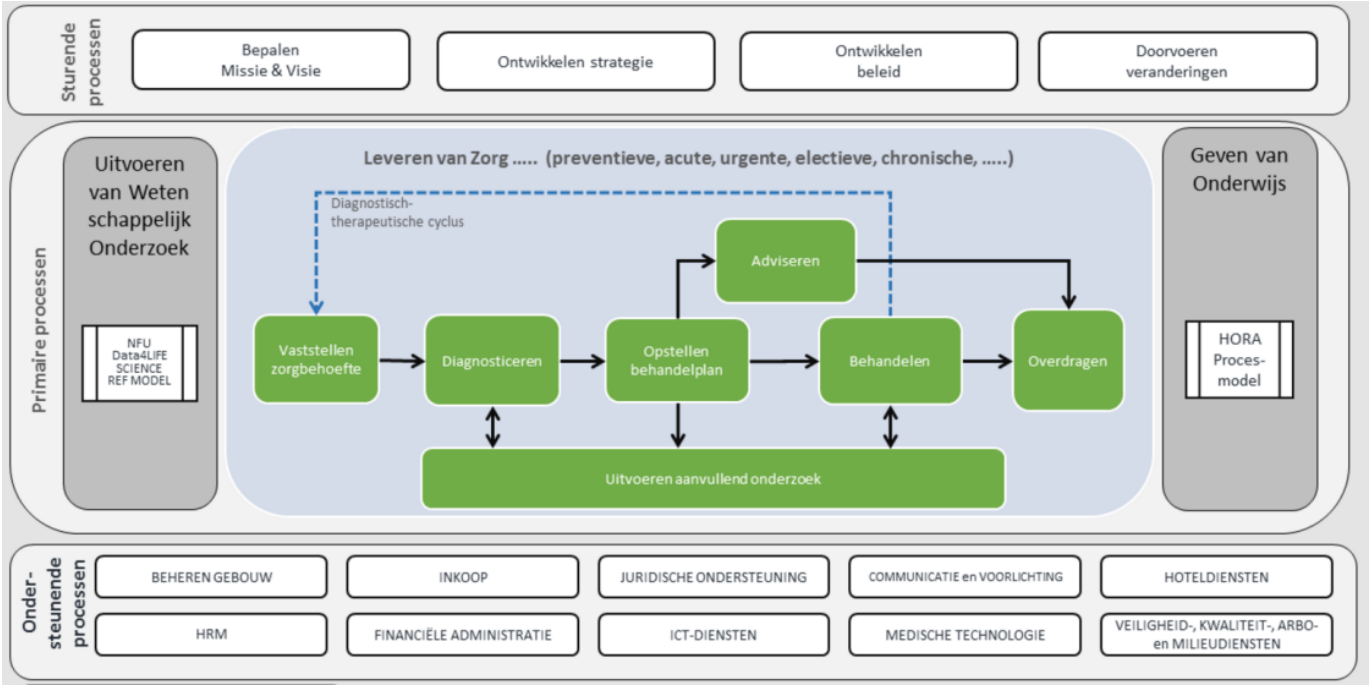
Figuur 2 Processen in de Zorg (Bureau HHM, 2011)

Toelichting

Deze processen zijn van toepassing op particuliere zorgorganisaties zoals individuele zorginstelling Lindenhout. De primaire processen in de zorg beginnen met een intake, waarbij er een cliëntdossier met daarin een zorgovereenkomst en zorgplan wordt opgesteld (Bureau HHM, 2011). In de zorgplanning wordt er vervolgens een planning gemaakt op basis van deze intake. In dit proces zijn de ondersteunende processen; personeelsplanning en financiën belangrijk. Vervolgens zal er zorg worden verleend naar aanleiding van het zorgplan zoals opgenomen in het cliëntendossier. Na het verlenen van de zorg wordt er geëvalueerd over de zorgvraag en de zorgverlening. De kans dat bij het gebruik van smartapparatuur in het bedrijfsnetwerk een proces verstoord wordt is aanwezig. Wanner een kwaadwillende het bedrijfsnetwerk binnen kan dringen en bij informatie over cliënten kan komen, dan kan de kwaadwillende deze informatie aanpassen of versleutelen. Wanneer deze informatie ontbreekt, kan de zorgverlening niet meer plaatsvinden. De zorgsector heeft te maken met cybercriminelen als grootste dreiging (Nationaal Cyber Security Centrum, 2016). Volgens het cybersecuritybeeld 2016 zijn er phising-e-mails en

ransomware verstuurd. Deze waren gericht op het verkrijgen van inloggegevens. Het grootste gevaar voor de zorgcontinuïteit is het onbewust lekken van informatie door interne medewerkers. Wanneer hier sprake van is, kunnen cybercriminelen het zorgproces verstoren.

Processen ziekenhuizen



Figuur 3 Procesmodel Ziekenhuis (Ziraonline, 2016)

Toelichting

In figuur 3 zijn de primaire processen en ondersteunende (secundaire) processen zichtbaar van ziekenhuizen. Het primaire proces loopt van het vaststellen van de zorgbehoefte tot het behandelen van de patiënt (Ziraonline, 2016). Na behandeling vindt de overdracht plaats. In het model zijn de ondersteunende processen te zien, die nodig zijn om het leveren van zorg mogelijk te maken. Er zijn veel plekken in het bedrijfsproces die kwetsbaar zijn. In dit onderzoek wordt er gekeken naar patiëntveiligheid, wat als één van de belangrijkste onderwerpen in ziekenhuizen kan worden beschouwd. Het onderwerp valt onder het ondersteunende proces veiligheid, kwaliteit, arbo en milieudiensten (VMSzorg, 2017). Volgens VMS-Zorg zijn de volgende thema's belangrijk bij het waarborgen van de patiëntveiligheid:

- voorkomen van wondinfecties na een operatie;
- voorkomen van lijnsepsis en behandeling van ernstige sepsis;
- vroege herkenning en behandeling van de vitaal bedreigde patiënt;
- medicatieverificatie bij opname en ontslag;
- kwetsbare ouderen;
- voorkomen van nierinsufficiëntie bij intravasculair gebruik van jodiumhoudende middelen;
- voorkomen van verwisseling bij en van patiënten;
- voorkomen van incidenten bij high-risk medicatie;
- voorkomen van onnodig lijden van patiënten door pijn;
- optimale zorg bij acute coronaire syndromen.

Volgens VMS-Zorg is het de bedoeling dat de patiëntveiligheid wordt gewaarborgd en de onbedoeld vermijdbare schade in ziekenhuizen terug wordt gedrongen. Dit gebeurt door middel van het verbeteren van de hierboven genoemde thema's. Patiënten lopen risico doordat onder andere patiëntgegevens, medicijngebruik en voedselaanbod vaak digitaal wordt geregeld. Er bestaat een kans dat deze gegevens

aangepast of versleuteld kunnen worden door cybercriminelen. Dit kan gebeuren wanneer de kwaadwillenden via smartapparatuur in het bedrijfsnetwerk kunnen komen en bij de gegevens kunnen komen. Er is een kans dat deze gegevens aangepast of versleuteld worden waardoor een patiënt de verkeerde voeding of medicijnen krijgt. Dit kan leiden tot levensbedreigende situaties. Wanneer patiëntgegevens niet correct zijn of missen dan kan er verkeerde zorg worden verleend wat kan leiden tot een dodelijke afloop.

2.7 Adviesproduct

Nadat de risico's van de smartapparatuur in kaart zijn gebracht, is er een adviesproduct ontwikkeld. Dit product is een checklist geworden waar de risico's in terug te vinden zijn. In overleg met de afdeling marketing van Sincerus, is er bepaald waar het adviesproduct aan moet voldoen. In het adviesproduct ontbreken de onderdelen risico's en maatregelen in ieder geval niet.

2.8 Relevante wetgeving

Dat cybercriminaliteit onder misdrijven valt, is te zien in het Wetboek van Strafrecht. Naast de Wet bescherming persoonsgegevens zijn de volgende wetsbepalingen, die betrekking hebben op het binnendringen van computersystemen, uit het Wetboek van Strafrecht relevant voor dit onderzoek.

Artikel 138 ab Sr en **Artikel 138 b Sr** gaan over het onrechtmatig binnendringen ofwel belemmeren van computers en geautomatiseerd werk. De artikelen maken duidelijk welke straffen er volgen bij het plegen van deze misdrijven. Deze wetten zijn relevant voor het onderzoek omdat het ook van toepassingen is op het binnendringen van smartapparatuur.

Artikel 161sexies Sr en **Artikel 161septies Sr** gaan over dat enig geautomatiseerd werk of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar wordt gemaakt, dat een stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld. De artikelen maken duidelijk welke straffen er staan op deze misdrijven. Deze wetten zijn relevant omdat in dit onderzoek onder andere wordt gekeken naar risico's van smartapparatuur waarbij bedrijfsprocessen gevaar lopen.

Artikel 317 Sr, **Artikel 318 Sr** en **Artikel 350 a t/m d Sr** zijn relevante artikelen omdat deze wat zeggen over afpersing en het dwingen tot afgifte van gegevens. De artikelen gaan ook over het onbruikbaar, ontoegankelijk maken of wissen van gegevens die door middel van geautomatiseerd werk zijn opgeslagen. Het is mogelijk dat kwaadwillenden, via smartapparatuur, bij gevoelige gegevens kunnen komen en deze kunnen aantasten.

2.9 Relevante ISO-Normen

Er zijn verschillende normen die worden beheerd. Zo zijn er nationale normen (NEN), Europese Normen (EN) en Internationale normen (ISO, IEC). Deze normen zijn bedoeld om te normaliseren. De volgende normen zijn relevant voor dit onderzoek en kunnen waardevolle informatie bevatten:

NEN-EN-ISO 22301- Norm voor Business Continuity Management System

Dit is een internationale norm voor de inrichting en beheer van een Business Continuity Managementsysteem. Dit systeem benadrukt de behoeften en noodzaak van een organisatie om beleid en doelstelling voor bedrijfscontinuïteit vast te stellen. De norm geeft ook richtlijnen voor het implementeren en uitvoeren van beheersmaatregelen, die ervoor zorgen dat een organisatie verstorende incidenten kan managen (CEN, 2014). Deze norm is relevant, omdat er in dit onderzoek wordt gekeken naar risico's die de bedrijfscontinuïteit kunnen aantasten.

ISO2022317- Norm voor het uitvoeren van een Business Impact Analyse

Deze internationale norm geeft details weer over hoe een Business Impact Analyseproces uitgevoerd moet worden als onderdeel van het Business Continuity Managementsysteem. Een business impact

analyse is een proces waarbij de gevolgen van verstorende incidenten worden geanalyseerd. Met deze norm kan de kwaliteit van dit proces worden geoptimaliseerd (SIS, 2015). Deze norm is op een ondersteunende manier goed te gebruiken om vast te kunnen stellen wat de impact is van het stilleggen van kritische bedrijfsprocessen.

ISO27001 De norm voor het Information Security Management System
Deze internationale norm is opgesteld om te voldoen aan de eisen voor het vaststellen, bieden, implementeren, het behouden en constante verbeteren van een informatiebeveiligingssysteem. De norm kan door interne en externe partijen worden gebruikt om de informatiebeveiliging te beoordelen. Het is een borgingsinstrument om de informatiebeveiliging te beheren en te verbeteren (ISO-IEC, 2013). Deze norm geeft relevante informatie over waar een informatiebeveiligingssysteem aan moet voldoen. Wanneer deze van hoge kwaliteit is, zal een organisatie minder risico lopen bij het gebruik van smartapparatuur in het bedrijfsnetwerk.

ISO/IEC 27032 Guide Lines For Cybersecurity
Dit is een internationale norm die richtlijnen biedt voor het verbeteren van de cybersecurity. Deze norm is afhankelijk van andere veiligheidsdomeinen zoals: informatiebeveiliging, netwerkbeveiliging, veiligheid van het internet en bescherming van de kritieke informatie-infrastructuur. Het geeft een overzicht van de cybersecurity, een verklaring van de relaties tussen cybersecurity en andere vormen van veiligheid, belanghebbenden en beschrijving van hun rol, richtlijnen voor de aanpak van cybersecuritykwesties en een kader die belanghebbenden in staat stelt samen te werken bij het oplossen van problemen met cybersecurity (ISO-IEC, 2012). Deze norm biedt ondersteuning bij het onderzoek, omdat de informatie over informatiebeveiliging relevant kan zijn.

NEN7510 Medische informatica- informatiebeveiliging in de zorg
Deze norm geeft hulpmiddelen en richtlijnen voor het juist gebruiken van informatiebeveiliging in de zorgsector (NEN, 2011). De organisaties waarvoor deze norm is bedoeld, variëren van individuele zorginstellingen tot grote zorginstellingen en ziekenhuizen. In deze norm staan onder andere maatregelen vermeld, die organisaties moeten treffen voor goede informatiebeveiliging. Daarnaast staat er ook in vermeld hoe deze te handhaven zijn en hoe je de informatiebeveiliging technisch en organisatorisch bepaalt.

3. Verantwoording onderzoeksmethode

Om de onderzoeksvragen en de probleemstelling te k beantwoorden was er informatie nodig. Deze informatie kon worden verkregen via verschillende methodes. Deze methodes worden in dit hoofdstuk uiteengezet.

3.1 Onderzoeksmethodes

Voor dit onderzoek zijn er meerdere onderzoeksmethodes gehanteerd. Om de nodige informatie over het onderwerp te bemachtigen, is er gebruik gemaakt van deskresearch en literatuuronderzoek. Deze informatie is belangrijk bij het beantwoorden van de probleemstelling en onderzoeksvragen. De benodigde informatie is verkregen via het internet en uit verschillende literatuur. Daarnaast is er kwalitatief onderzoek toegepast in de vorm van diepte-interviews met experts. De experts zijn geraadpleegd om meer zicht te krijgen op de risico's van smartapparatuur. Er zijn tien verschillende experts benaderd, waarvan er uiteindelijk zes hebben meegewerkt. Tijdens het verwerken van de interviewgegevens zijn er bestanden verloren gegaan van de interviews met Wouter Stol, René van den Nieuwenhoff en Robert Veenstra. Deze zijn daarom niet terug te vinden in de resultaten. Het interview met Harald Vranken is deels verloren gegaan, maar het deel wat bewaard is gebleven bevat wel bruikbare informatie. Er zijn ook organisaties uit de zorgsector geïnterviewd. In deze interviews is er besproken wat de rol van smartapparatuur in de organisaties is. Hiervan is het interview met Niels Drieënhuizen van

Lindenhout verloren gegaan. De informatie die nog te herinneren was, is in een verslag verwerkt. Dit verslag is teruggekoppeld naar de geïnterviewde.

Om te kijken welke risico's er verbonden zijn bij het gebruik van smartapparatuur in een organisatie, is er naast de interviews ook een risicoanalyse uitgevoerd via de koepelmethodiek. Deze methodiek is toegepast op het primaire zorgproces van de organisaties in de zorgsector. Als laatste zijn er afspraken gemaakt met de opdrachtgever Sincerus, welke beschikt over waardevolle kennis en informatie waarvan gebruik is gemaakt in het onderzoek. Zo is via gesprekken met de marketingafdeling van Sincerus onderzocht, hoe een adviesproduct eruit moet zien.

3.2 Dataverzamelingsmethode

Er is al aangegeven welke methoden van onderzoek er zijn toegepast. Deze methoden zijn deskresearch, literatuuronderzoek, het uitvoeren van een risicoanalyse en het houden van interviews. Bij de methode deskresearch is er gebruik gemaakt van de zoekmachine Google, waar betrouwbare bronnen op zijn gezocht. De bronnen die worden geraadpleegd zijn van lectoraten, onderzoeksbureaus en overheidsinstellingen. Naast deze bronnen zijn er ook bronnen gebruikt die over het onderwerp schrijven in de vorm van blogs of nieuws. Deze zijn alleen gebruikt wanneer er in meerdere blogs of sites dezelfde informatie is gevonden.

De volgende experts zijn geïnterviewd:

- Wouter Stol - Lector Cybersafety en bijzonder hoogleraar Politiestudies
- Harald Vranken – Universitair hoofddocent faculteit Management, Science & Technology Open Universiteit en Radboud Universiteit
- René van den Nieuwenhoff- Docent en onderzoeker Security Management Saxion
- Robert Veenstra - Security Professional Sincerus Consultancy B.V.
- Marielle Stoelinga - Associate Professor in Risk Management for Computer Systems Universiteit Twente
- Gea Wijn - Milieu- en BHV-Coördinator en ZIROP-beheerder Deventer Ziekenhuis

Uit de zorgsector zijn er verschillende organisaties benaderd, om te kijken wat de rol is van smartapparatuur binnen die organisatie. De volgende personen en organisaties hebben meegewerkt aan een interview over de rol van smartapparatuur in de organisatie:

- Incident en Problem manager, Lodewijk Huinink van Medisch Spectrum Twente
- Informatiemanager, Niels Drieënhuizen van Lindenhout
- Coördinator informatieveiligheid, Stephan Hazekamp van het St. Jansdal ziekenhuis
- Innovation manager, Jeroen Geerdink van Ziekenhuis Groep Twente

De interviewgegevens van zowel de organisaties als de experts zijn geanalyseerd met behulp van codeerschema's. Allereerst zijn de gegevens open gecodeerd en daarna zijn deze gegevens axiaal gecodeerd. Met behulp van het coderen zijn de resultaten overzichtelijker en is het makkelijker om verbanden te zien.

3.3 Validiteit en betrouwbaarheid

Bij wetenschappelijk onderzoek is het belangrijk dat deze betrouwbaar en valide is. Hieronder wordt er per onderzoeksvraag behandeld op welke manier dit is ingevuld.

1. **In welke mate speelt smartapparatuur een rol in de zorgsector?**

Bij het onderzoek is er gebruik gemaakt van vertrouwde sites en literatuur van onafhankelijke (overheids)instanties. De voor dit onderzoek geïnterviewde organisatiemedewerkers beschikken over een

beter beeld van de smartapparatuur dan iemand buiten de organisatie. Er is een kans dat de vier geïnterviewde organisaties niet representatief zijn voor de zorgsector. Wanneer er andere organisaties waren gekozen, was de uitkomst wellicht compleet anders. Er is geprobeerd om verschillende typen organisaties te benaderen. Zo krijg je niet alleen een beeld van één organisatie, maar wordt er een vergelijking gemaakt tussen meerdere organisaties. Hierdoor is het beeld van de rol van smartapparatuur in deze sectoren een stuk meer valide. Het begrip smartapparatuur is ook goed afgebakend, zodat er geen verwarring ontstaat tijdens het onderzoek.

2. **Welke risico's zijn er aanwezig bij het gebruik van smartapparatuur in het bedrijfsnetwerk en in welke mate zijn organisaties zich bewust van deze risico's?**

Via de koepelmethodiek afkomstig uit het 'Handboek Risicoanalysemethodieken' is er een risicoanalyse uitgevoerd waarbij de risico's van smartapparatuur in kaart zijn gebracht. Dit handboek is uitgegeven door het ministerie van Economische Zaken. Naast het uitvoeren van de risicoanalyse zijn er meerdere betrouwbare experts geraadpleegd. Naast deze experts zijn ook de organisatiemedewerkers geïnterviewd, om te kijken naar de risicobewustheid.

De koepelmethodiek laat zien welke risico's er spelen bij het gebruik van smartapparatuur in het bedrijfsnetwerk. Om ervoor te zorgen dat er op een correcte wijze onderzoek is uitgevoerd, is het onderzoek aangevuld met informatie van experts en ontwikkelaars. Sommige componenten die voor dit onderzoek niet van belang waren, zijn niet meegenomen. Naast deze twee onderzoekmethoden is er ook gebruik gemaakt van literatuuronderzoek.

3. **Waar moet een adviesproduct aan voldoen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector?**

De marketingafdeling van Sincerus heeft in een gesprek aangegeven wat de opdrachtgever zelf belangrijk vindt aan een adviesproduct. Zo voldoet een adviesproduct altijd aan de wensen van de opdrachtgever. Toen duidelijk was waar een adviesproduct aan moet voldoen, konden de aanbevelingen van het onderzoek worden verwerkt in een checklist waar in ieder geval de maatregelen en de risico's in zijn vermeld. Daarnaast zijn de maatregelen meegenomen die uit de interviews naar voren zijn gekomen.

3.4 Populatie en steekproef

Om ervoor te zorgen dat de onderzoekspopulatie niet te groot is, is ervoor gekozen om het onderzoek af te bakenen tot de zorgsector. Er is voor deze sector gekozen omdat de opdrachtgever meer inzicht wenste in deze sector. Daarnaast werd er voor het onderzoek verwacht dat er in deze sector veel smartapparatuur wordt gebruikt. Om een betrouwbare steekproef uit te kunnen voeren moest deze willekeurig en representatief zijn. De eenheden in de steekproef moesten wat betreft een aantal belangrijke kenmerken gelijk zijn aan de populatie. In dit onderzoek is er daarom gekozen voor vier organisaties in de zorgsector die willekeurig zijn, maar wel de sector representeren.

3.5 Operationalisatie

Onderzoeksvragen	Variabelen	Indicatoren	Onderzoeksmethode
1. In welke mate spelen *smartapparatuur* een rol in de zorgsector*?*	**Smartapparatuur**	Omschrijving definitie Welke van de volgende categorieën smartapparatuur spelen een rol in de zorgsector? Smart Domestic Appliances Smart Entertainment Smart Energy Smart Lightning Smart Motorization Smart Security	• Deskresearch • Literatuuronderzoek • Overleg met Sincerus • Interviews met medewerkers uit verschillende zorgorganisaties

		Smart Communication Smart Health De rol van smartapparatuur: types Aantal aanwezig Aantal in gebruik	
	Type organisaties	Ziekenhuizen Individuele zorginstelling	• Deskresearch • Overleg met Sincerus
2. Welke *risico's* spelen er bij het gebruik van *smartapparatuur* in het *bedrijfsnetwerk* en in welke mate zijn organisaties zich bewust van deze risico's?	**Risico's**	Kansen Blootstelling Impact	• Deskresearch • Risicoanalyse; 'Koepelmethodiek' toepassen op primaire zorgproces • Interviews met experts • Interviews bij zorgorganisaties • Risicoanalyse • ISO-normen gebruiken
	Smartapparatuur	Rol van smartapparatuur in de onderzochte sectoren	• Afhankelijk van deelvraag 1
	Bedrijfsnetwerk	Omschrijving definitie	• Deskresearch
3. Waar moet een *adviesproduct* aan voldoen om *advies* te kunnen geven over het gebruik van smartapparatuur in de zorgsector?	**Adviesproduct**	Kwaliteit adviesproducten Soorten adviesproducten	• Deskresearch • Overleg met de marketingafdeling van Sincerus
	Advies	Welke maatregelen moeten er getroffen worden	• Interviews met experts • Analyseren van de risicoanalyse

4. Resultaten

In dit hoofdstuk staan de resultaten van de onderzochte onderzoeksvragen. Deze resultaten zijn tot stand gekomen door middel van literatuuronderzoek, interviews, een risicoanalyse en deskresearch. De volgende vragen zijn onderzocht;

- In welke mate speelt smartapparatuur een rol in de zorgsector?
- Welke risico's zijn er aanwezig bij het gebruik van smartapparatuur in het bedrijfsnetwerk en in welke mate zijn organisaties zich bewust van deze risico's?
- Waar moet een adviesproduct aan voldoen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector?

4.1 In welke mate speelt smartapparatuur een rol in de zorgsector?

Om tot een antwoord te komen op de vraag of smartapparatuur een rol speelt in de zorgsector, zijn er interviews uitgevoerd bij vier organisaties in de zorgsector. Er is onderzocht in hoeverre de organisaties bekend zijn met het begrip smartapparatuur, of er in de organisaties smartapparaten worden gebruikt, welke soorten smartapparatuur de organisaties gebruiken en/of de organisaties enig beleid hebben ten aanzien van het gebruik van smartapparatuur in de organisatie. De resultaten van deze componenten geven een beeld weer van de rol van smartapparatuur in de zorgsector. De volgende organisaties hebben meegewerkt aan het onderzoek:

- Medisch Spectrum Twente: dit ziekenhuis is gevestigd in Enschede en heeft enkele poliklinieken in Oldenzaal, Haaksbergen en Losser. Het is een grote organisatie, waar bijna alle soorten specialismes worden aangeboden. Het is een ziekenhuis die topklinische zorg aanbiedt. Daarnaast biedt het ziekenhuis op een aantal terreinen ook zorg die normaal alleen in academische ziekenhuizen worden aangeboden. Daarnaast is het ziekenhuis een traumacentrum voor een groot gedeelte van Oost-Nederland en een gedeelte van Duitsland (Medisch spectrum Twente, 2017).
- St. Jansdal: het St. Jansdal is een middelgroot ziekenhuis in Harderwijk, waar een breed pakket aan zorg wordt aangeboden. Het ziekenhuis heeft 150 medewerkers, 340 vrijwilligers en 120 specialisten. Bijna alle specialismen worden hier aangeboden (St. Jansdal, 2017).
- Ziekenhuisgroep Twente: dit is een ziekenhuis met locaties in Almelo en Hengelo. Daarnaast zijn buitenpoliklinieken in Goor, Geesteren, Rijssen, Nijverdal en Westerhaar onderdeel van de organisatie. Jaarlijks worden er zo'n 250.000 patiënten behandeld door 3.200 medewerkers en 220 medisch specialisten (ZGT, 2017).
- Lindenhout: is een individuele zorginstelling die jeugdzorg aanbiedt in meerdere regio's in Gelderland en in Overijssel. De organisatie bestaat uit 360 medewerkers die hulp bieden aan meer dan 3500 cliënten. Er wordt veel ambulante hulp geboden aan 1000 kinderen die opgroeien in pleeggezinnen. Daarnaast worden er ook 350 kinderen opgevangen in gezinshuizen (Lindenhout, 2016).

De resultaten van de interviews met deze organisaties worden hieronder weergegeven. Deze resultaten zijn aangevuld met literatuuronderzoek en bevindingen van geïnterviewde experts.

4.1.1 Bekendheid organisaties met smartapparatuur

Aan de organisaties is gevraagd of ze bekend zijn met de term smartapparatuur. De antwoorden zijn bij alle organisaties verschillend. De ene organisatie antwoordde dat de organisatie beginnend bekend is, een andere organisatie antwoordde dat de organisatie minder bekend is, een organisatie antwoordde dat de organisatie van het bestaan afweet maar het nog niet gebruikt en de laatste organisatie is er redelijk bekend mee. Uit deze antwoorden blijkt dat de organisaties er wel iets van afweten, maar nog niet genoeg. Expert Vranken zegt dat iedereen er notie en kennis van heeft (Vranken, 2017). Expert Stoelinga

zegt over de bekendheid van smartapparatuur in de zorg: ''*Ik denk dat de zorgsector weet dat het bestaat, maar erg huiverig is om het in te voeren. Invoeren in een organisatie is niet zo gemakkelijk. Thuis koop je gewoon een smartthermostaat en ben je klaar. In een ziekenhuis moet de gehele organisatie zich richten op die smartprocessen. Die moeten heel goed ingebed worden in de hele workflow van een organisatie. Er zijn allerlei protocollen, want een ziekenhuis is ontzettend geprotocolleerd. Als je iets 'smarts' wil doen moet je kijken of de protocollen nog voldoende zijn, adequaat zijn, of dat er veranderingen in moet komen. Er moet over nagedacht worden, het moet goedgekeurd worden en iedereen moet er zijn zegje over doen.*'' (Stoelinga, 2017)De organisaties in de zorgsector zijn bekend met smartapparatuur. Nu is het van belang om te kijken of de organisaties zelf ook smartapparatuur gebruiken.

4.1.2 Gebruik smartapparatuur in de organisaties

De vier ondervraagde organisaties zijn bekend met smartapparatuur, maar volgens Stoelinga wordt er nog niet veel gebruik van gemaakt in de zorgsector (Stoelinga, 2017). Uit de interviews met de organisaties blijkt dat er in de drie onderzochte ziekenhuizen smartapparatuur wordt gebruikt. In de individuele zorginstelling Lindenhout, wordt er ook gebruik gemaakt van smartapparatuur, maar in een veel mindere mate. Dit verschil komt onder andere doordat de onderzochte ziekenhuizen veel gebruik maken van smart health en de individuele zorginstelling niet. Uit het interview met Stephan Hazekamp van het St. Jansdal ziekenhuis, blijkt dat 20 tot 30% van alle medische apparatuur in het St. Jansdal ziekenhuis smart is. Deze categorie smartapparatuur komt het meest voor in dit ziekenhuis.

Naast smartapparatuur wordt er in de zorgsector ook gebruikt gemaakt van andere Internet of Things-toepassingen zoals computers, tablets en smartphones. Volgens een onderzoek van netwerkleverancier Aruba Networks, gebruikt 60% van alle zorgorganisaties wereldwijd op enige wijze Internet of Things-toepassingen in de organisatie (Poel, 2017). Wanneer het gaat om het implementeren van deze IoT-toepassingen, is volgens Aruba Networks de zorgsector de op twee na geavanceerdste sector (Kregting, 2017). Dit onderzoek laat zien dat er in de zorgsector veel gebruik wordt gemaakt van onder andere smartapparaten, computers, tablets en smartphones. Nu duidelijk is dat er in de zorgsector gebruik wordt gemaakt van smartapparatuur, kan er worden gekeken naar welke typen smartapparatuur er gebruikt wordt gemaakt.

4.1.2.1 Typen smartapparatuur in de organisaties

Type smartapparatuur	Aantal
Slimme wasmachines	2
Slimme koelkasten	1
Smart-tv	4
Slimme thermostaat	2
Slimme meters	1
Slimme verlichting	2
Slimme lampen	1
IoT-sensoren	1
Slimme liften	1
Slimme deuren	1
Slimme sloten	2
Smart alarm	1
Smartwatches	4
Medisch oproepsysteem	1
Smart plansysteem	1
Pacemakers	2
Infusiepompen	2
Overige smart health	2

Tabel 1 Type smartapparatuur

De vier onderzochte organisaties is een lijst met smartapparatuur voorgehouden met veelvoorkomende apparatuur. Daarnaast was er gelegenheid tot eigen inbreng vanuit de organisaties. In tabel 1 is te zien, welke apparaten van de voorgelegde lijst door de zorgorganisaties zijn genoemd en hoe vaak deze zijn genoemd. Zo is te zien dat er in alle vier de organisaties smart-tv's en smartwatches voorkomen. Er zijn verschillende apparaten die een of twee keer voorkomen. De smartapparaten die wel op de voorgestelde lijst staan maar niet zijn genoemd, zijn niet meegenomen in de tabel. Uiteindelijk zijn er zestien verschillende soorten smartapparatuur genoemd. Lodewijk Huinink van medisch Spectrum Twente en Stephan Hazekamp van het St. Jansdal ziekenhuis gaven beide aan, dat er veel smart-tv's aanwezig zijn in de eigen organisatie. Bij beide organisaties gaat het om ongeveer twintig smart-tv's. Niels Drieënhuizen van Lindenhout gaf aan dat er in de gehele organisatie slechts één smart-tv aanwezig is (Drieënhuizen, 2017). Alle zorgorganisatiemedewerkers konden geen antwoord geven op de vraag: in welke hoeveelheid komt smartapparatuur voor in de organisatie? Deze informatie hebben de organisaties zelf wel tot hun

beschikking. Er kan wel een beeld worden geschetst welke IoT-toepassingen het meest worden gebruikt. Volgens het onderzoek van 'Aruba Networks' worden wereldwijd in de zorgsector namelijk de volgende categorieën IoT-toepassingen het meest gebruikt:

- 64% Patiëntmonitors
- 56% Energievoorzieningen
- 33% X-rays en beeldapparatuur (Aruba Networks, 2017).

Nu duidelijk is welke smartapparatuur er wordt gebruikt in de zorgsector, is het de vraag of de organisaties weten hoe er met deze apparatuur moet worden omgegaan. Voeren organisaties een bepaald beleid omtrent het gebruik van smartapparatuur of de aanschaf daarvan?

4.1.3 Beleid ten aanzien van het gebruik van smartapparatuur in de organisaties

Aan de vier zorgorganisatiemedewerkers is gevraagd of er enig beleid is omtrent het omgaan met smartapparatuur in de eigen organisatie. De organisaties voeren allemaal een beleid wat betreft algemene informatiebeveiliging, alleen niet specifiek voor smartapparatuur. Smartapparatuur valt voor een deel onder algemene informatiebeveiliging. Bij de aanschaf wordt er bij alle onderzochte ziekenhuizen een standaard risicoanalyse uitgevoerd, waarna vervolgens de impact van het nieuwe apparaat wordt bepaald. Alle ondervraagde organisaties kunnen daarna in een overzicht zien, welke apparaten er allemaal in verbinding staan met het bedrijfsnetwerk. Er is in het kader van, hoe er met de smartapparatuur wordt omgegaan, gevraagd of de standaardwachtwoorden van nieuwe smartapparatuur worden aangepast. Alle ondervraagde organisaties kunnen niet met zekerheid zeggen of dit het geval is. Dit laat zien dat er weinig tot geen beleid is, wat betreft het veranderen van de wachtwoorden van deze apparaten.

4.2 Welke risico's zijn er aanwezig bij het gebruik van smartapparatuur in het bedrijfsnetwerk en in welke mate zijn organisaties zich bewust van deze eventuele risico's?

In de vorige paragraaf is duidelijk geworden dat smartapparatuur een rol speelt in de zorgsector. Het is nu interessant om te kijken of er ook risico's kleven aan het gebruik van smartapparatuur in een bedrijfsnetwerk, welke impact die risico's hebben en/of organisaties zich daarvan bewust zijn. Deze onderzoeksvraag is beantwoord door middel van interviews met experts, interviews met zorgorganisatiemedewerkers, een risicoanalyse en aanvullend literatuuronderzoek. Allereerst is het van belang om de definitie van een bedrijfsnetwerk af te bakenen voordat de risico's bij het gebruik van smartapparatuur in het bedrijfsnetwerk in kaart kunnen worden gebracht. Een bedrijfsnetwerk is een koppeling van meerdere computers in één organisatie, waardoor deze gegevens kunnen uitwisselen (Van Beurden, 2014). Nu dit bekend is kunnen de overige resultaten worden benoemd.

Allereerst worden de risico's afkomstig uit de interviews weergegeven om vervolgens te worden aangevuld met informatie uit betrouwbare bronnen. Hierna wordt er uiteengezet wat de impact van deze risico's zijn, daarna wordt het risicobewustzijn uitgewerkt en tot slot worden de resultaten van de risicoanalyse weergegeven.

4.2.1 Risico's

De risico's van het gebruik van smartapparatuur in het bedrijfsnetwerk zijn onderverdeeld in de volgende categorieën:

- technische risico's;
- privacy risico's;
- gebruiksrisico's.

4.2.1.1 Technische Risico's

Elke technische ontwikkeling brengt risico's met zich mee (Van Rijsewijk, 2016). Volgens Van Rijsewijk wordt de informatietechnologie opener en steeds meer met elkaar verbonden, wat betekent dat het ook steeds kwetsbaarder is voor aanvallen. Van Rijsewijk (2016) zegt: *''Precies datgene wat digitale technologie waardevol maakt, maakt het ook kwetsbaar''* (p.32). De volgende technische risico's spelen bij het gebruik van smartapparatuur in het bedrijfsnetwerk:

Laag niveau van beveiliging: doordat de smartapparatuur een nieuw product is, is de beveiliging nog niet optimaal. Stoelinga (2017) zegt daarover: *''Nou, er moet wel wat gebeuren. Er moeten hierboven zich wel mensen druk over gaan maken. Als iedereen denkt; het loopt wel los en over vijf jaar is het probleem vanzelf opgelost. Dat is niet zo. Dan kunnen er wel echt ongelukken gebeuren.*'' Stoelinga (2017) zegt ook het volgende: ''*Het nare van Internet of Things, er zijn zoveel ingangen op het internet. Je hoeft maar één ingang te hebben en dan kan je via het ene device naar het andere device, totdat je bij allerlei kritische systemen kunt komen.''* Uit het interview met Stoelinga (2017) is ook gebleken dat de algemene mening over de beveiliging van smartapparatuur is, dat de beveiliging zo lek als een mandje is. Vranken (2017) zegt hierover: *''Er is in sommige devices überhaupt geen security te bespeuren. Bij andere devices zijn er wel securitymaatregelen genomen, maar daar zitten manco's aan. Neem bijvoorbeeld een apparaat waartoe toegang is geregeld met een wachtwoord, maar het is een default wachtwoord wat makkelijk te raden is en algemeen bekend is. Het is moeilijk om dat wachtwoord aan te passen, of het kan alleen maar als je de firmware aanpast. Er zitten wel securitymaatregelen in, maar in de praktijk zijn die makkelijk te omzeilen. Hierdoor is er niet echt sprake van beveiliging.*"
KPN CISO Baloo deelt deze mening dat de apparatuur vaak te hacken is doordat deze in de default-stand staan. Andere redenen zijn dat de wachtwoorden eenvoudig zijn of de software niet geüpdatet is (Computable, 2017). De FBI (Federal Bureau of Investigation) zegt ook dat de beveiliging onvoldoende is, waardoor kwaadwillenden op afstand spam kunnen versturen of persoonlijke informatie kunnen stelen (FBI, 2015). Volgens James Lyne, directeur van de onderzoeksafdeling, gaat de beveiliging van IoT-apparatuur tien jaar terug in de tijd (Lacroix, 2017). De beveiliging is dus ook volgens Lyne nog niet op een hoog niveau. Lyne geeft aan dat met zulke slechte beveiliging het een kwestie van tijd is tot zich een ramp volstrekt. De redenen hiervoor liggen volgens de experts bij de producenten.

Beveiliging wordt niet meegenomen in het productieproces: producenten van smartapparatuur ontwikkelen security nog niet mee in de design-fase (The Datacentergroup, 2016). Volgens The Datacentergroup gebruiken de apparaten vaak standaard codes, die makkelijk te hacken zijn. Stoelinga (2017) gaf het volgende aan over de productie van smartapparatuur: *''Er is heel veel druk om een korte 'time-to-market' te hebben en als eerste een product op de markt te brengen. Er is gewoon geen tijd voor securityreviews en gedegen beveiliging. Wat mensen gaan doen is het volgende; ze nemen een oud device, ze stoppen er wat sensoren in, stoppen er een marketingsausje overheen en klaar. Dat is natuurlijk heel wat anders dan wat je moet doen om het allemaal beveiligd te krijgen.''* Vranken (2017) gaf het volgende aan over de al dan niet aanwezige problematiek bij de producent: *''Dat zou ik niet zo durven zeggen. Ik denk dat het verschilt per product en waar die voor bedoeld is. In de consumermarkt wordt er minder zwaar aan beveiliging getild, dan bij apparaten die in kritische infrastructuur worden gebruikt. Bij de apparaten die daarvoor bedoeld zijn, zijn zwaardere securitymaatregelen genomen.''*
De slechte beveiliging ligt volgens Vranken en Stoelinga dus aan de consumentenmarkt en de druk om als eerste een product op de markt te brengen. Volgens Lyne wordt veel apparatuur zo goedkoop mogelijk geproduceerd, dit heeft als gevolg dat de software die op de apparaten wordt gezet, niet kan worden geüpdatet. Lyne, zegt net als Vranken, dat door firmware-updates dit soms wel kan worden opgelost. Echter, kunnen sommige apparaten niet worden geïntegreerd in de hardware of softwarebescherming, waar organisaties zichzelf mee tegen aanvallen beschermen. Daarnaast is, volgens Lyne, de variatie van de

verschillende producten een uitdaging. De apparatuur zorgt voor veel nieuwe data op het bedrijfsnetwerk, wat allemaal beheerd en beveiligd moet worden.

Veel smartapparaten worden in grote hoeveelheden geproduceerd: dit betekent dat de apparaten bijna identiek aan elkaar zijn en ook op dezelfde manier functioneren. Wanneer er een beveiligingsrisico in een van de producten zit, is aan te nemen dat deze in al deze apparaten is terug te vinden. Kwaadwillenden kunnen op deze manier meerdere smartapparaten hacken, omdat deze allen dezelfde kwetsbaarheden bevatten (Chapin, Eldridge, & Rose, 2015).

Smartapparatuur heeft een lange levensduur: volgens Chapin, Eldrige en Rose wordt smartapparatuur zo ontwikkeld dat deze vaak langer mee gaat dan normale hightech apparatuur. Dit kan betekenen dat het apparaat het langer overleeft dan de producent van het product. Het is dan moeilijk om ze nog te updaten of te upgraden. De software krijgt geen nieuwe updates meer en dan kan de beveiliging niet voldoende zijn voor de gehele levensduur. Dit betekent dus dat de lange termijn ondersteuning een uitdaging is.

Smartapparatuur heeft soms geen mogelijkheid tot updates: Chapin, Eldrige en Rose zeggen dat sommige smartapparatuur zelfs zo zijn ontworpen dat er geen mogelijkheid is tot het uitvoeren van updates. Hierdoor moeten de updates door de gebruiker zelf worden toegevoegd wat ongemak veroorzaakt. Dit maakt een apparaat kwetsbaar voor hackaanvallen.

Smartapparatuur staat altijd in verbinding: volgens Lacroix staan smartapparaten altijd aan en in verbinding. De apparaten hoeven eenmalig een authenticatieproces te doorlopen (Lacroix, 2017). De gateways waarmee de apparaten op het bedrijfsnetwerk zitten, zijn hierdoor ook kwetsbaar. Deze moeten beter worden beveiligd om het risico op infiltratie te verkleinen. De FBI voegt daaraantoe dat smartapparatuur verbinding kan maken met het internet, zonder dat er menselijke interactie nodig is (FBI, 2015).

4.2.1.2 Privacy risico's

Smartapparatuur bevat naast de technische risico's, ook een aantal privacy risico's. Het apparaat verzamelt gegevens uit de omgeving die betrekking hebben op mensen (Chapin, Eldridge, & Rose, 2015). Volgens Chapin, Eldrige en Rose zijn deze gegevens nodig om het apparaat in het voordeel van de gebruiker te laten werken. Deze gegevens zijn vaak ook beschikbaar voor de fabrikant of leverancier van het apparaat. Dit wordt een probleem wanneer de gebruiker andere privacy verwachtingen heeft dan de producent. De volgende risico's spelen als het gaat om privacy:

Apparaten kijken en luisteren mee: Chapin, Eldrige en Rose geven aan dat sommige smartapparaten spraakherkenning of visiefuncties bevatten. Hierdoor kan de situatie ontstaan dat bijvoorbeeld een smart-tv, voortdurend naar gesprekken meeluistert of meekijkt naar een activiteit. Deze gegevens worden dan selectief doorgestuurd naar een Cloud waar soms ook een derde partij bij kan.

Geen gebruikersinterface om privacy voorwaarden te accepteren: Chapin, Eldrige en Rose zeggen dat de gebruikers soms geen mogelijkheid hebben om de privacy voorwaarden te accepteren, zoals bij een computer of een smartphone wel het geval is. Dit komt doordat er op smartapparatuur vaak geen gebruikersinterface zit, wat betekent dat gebruikers geen controle hebben over de manier waarop persoonsgegevens worden gebruikt en verzameld. Hierdoor ontstaat er een kloof tussen de privacy voorkeuren van de gebruiker en smartapparatuur die de gegevens verzamelt.

Gebruik in de privésfeer: er zijn volgens Chapin, Eldrige en Rose ook verschillen tussen publieke ruimtes en privéruimtes wat betreft privacy. In publieke ruimtes verwachten gebruikers sneller dat de apparatuur gegevens opslaat en dit wordt door de gebruikers eerder geaccepteerd. In de privésfeer verwachten gebruikers dit in mindere mate en ervaren dit ook als minder prettig. In de praktijk zal smartapparatuur in beide gevallen evenveel gegevens verzamelen. Dit betekent dat de gebruiker dit niet altijd doorheeft in de privésfeer of wanneer het wordt gebruikt in een organisatie.

Gebruiker heeft geen zicht op welke gegevens er worden verwerkt: Chapin, Eldrige en Rose geven aan dat de gebruiker niet altijd zicht heeft welke gegevens de smartapparatuur precies verwerkt. Dit is een privacy risico, omdat een apparaat meer gegevens kan verwerken dan een gebruiker doorheeft. De producent kan ook updates geven zonder dat de gebruiker dit door heeft.

4.2.1.3 Gebruiksrisico's

Naast de technische risico's en de privacy risico's, zijn er ook risico's met betrekking hoe de gebruiker met de smartapparatuur om dient te gaan. Hoe mensen met smartapparatuur omgaan kan veel uitmaken. Volgens van Rijsewijk wordt de organisatie kwetsbaarder naar mate het vertrouwen in de werknemer toeneemt. Er is altijd kans dat medewerkers fouten maken en verkeerd met de apparatuur omgaan. Controle beperkt de kans op fouten, maar het motiveert niet. Volgens Stoelinga (2017) is security erg onhandig. Het is niet gebruikersvriendelijk en elke maatregel is extra lastig. Het is het handigst wanneer alles gewoon bereikbaar is zonder te veel gedoe, maar zo zit het niet in elkaar. De risico's die spelen bij het gebruik van smartapparatuur afkomstig uit de interviews zijn:

- medewerkers willen zo snel mogelijk bij patiëntgegevens;
- medewerker is niet bereid veel wachtwoorden in te voeren;
- standaardwachtwoorden worden niet veranderd;
- medewerkers denken dat andere organisaties eerder worden getroffen dan de eigen organisatie;
- er hebben zich nog geen echte incidenten voorgedaan dus er hoeven nog geen veiligheidsmaatregelen te worden getroffen;
- medewerkers zijn minder bereid om regels na te leven;
- security wordt omzeild uit gemak;
- wie kan er allemaal op inloggen? Systeembeheerders zijn in principe de laatsten die erbij kunnen komen. Daar schuilt een risico in.

Social Engineering: naast deze risico's speelt er nog iets anders, namelijk Social Engineering. Dit is een gebruikersrisico omdat de gebruiker (mens) wordt aangevallen als zwakste schakel (Leukfeldt, van Eekelen, de Jong, & Vranken, 2012). Volgens Leukfeldt, van Eekelen, de Jong en Vranken zijn kwaadwillenden op wachtwoorden of andere persoonlijke informatie uit. Kwaadwillenden doen zich bijvoorbeeld voor als iemand van de IT-helpdesk en proberen zo wachtwoorden te ontfutselen bij de nietsvermoedende gebruiker. Dit kan ook bij smartapparatuur worden toegepast. Wanneer de kwaadwillende achter het wachtwoord komt van smartapparatuur, dan kan die daarop inloggen en zo in het bedrijfsnetwerk komen, wat grote gevolgen kan hebben. Naast deze gebruikersrisico's zijn er ook nog bijzondere risico's die expliciet in de zorgsector voorkomen.

Informatiebeveiliging heeft geen prioriteit: volgens Stoelinga wordt er in de zorgsector niet altijd de juiste urgentie gegeven aan informatiebeveiliging. Stoelinga (2017) zegt: *''Het management van ziekenhuizen zijn vaak medisch geschoolde mensen, die de meeste affiniteit hebben met waar hun core-expertise ligt. Daar ligt het ook aan.''* Het kan worden opgelost door mensen aan te nemen die er wel verstand van hebben maar volgens Stoelinga is het niet zeker dat ze doordrongen zijn van de ernst.
De beschikbaarheid van data speelt volgens Stoelinga ook een grote rol. De arts zit niet te wachten om nog drie wachtwoorden in te voeren wanneer een patiënt met spoed een operatie moet worden uitgevoerd. De arts wil meteen het medisch profiel van de patiënt kunnen zien (Stoelinga, 2017).

4.2.4 Impact

Nu de risico's van het gebruik van smartapparatuur bekend zijn, is het van belang om te weten wat de impact is. De impact van de risico's bij het gebruik van smartapparatuur is hetzelfde als bij andere beveiligingsrisico's (Stoelinga, 2017). Volgens Stoelinga lopen patiëntdata en de privacy van de patiënten gevaar. De risico's kunnen ook uitval van de systemen veroorzaken. Een ziekenhuis kan makkelijk plat worden gelegd. Stoelinga (2017) zegt: *''Risico's zijn zeldzaam, ze hebben wel een hoge impact en het gemak is groot. Het is dus erg verleidelijk om te denken dat niet ik, maar mijn buurman wordt*

aangevallen.'' Lodewijk Huinink van Medisch Spectrum Twente zegt ook dat het beïnvloeden van patiëntdata het belangrijkste gevolg is van de risico's. De patiëntveiligheid loopt hierdoor gevaar. Expert Gea Wijn zegt dat het afhankelijk is per patiënt of die een groot risico loopt bij verandering van patiëntdata. Gea Wijn (2017) zegt het volgende: *''Als de patiënt hier ligt dankzij een knieoperatie zal deze niet zuurstofafhankelijk zijn. Als deze patiënt geen diëten heeft en deze krijgt therapie, eten en drinken, dan kan er niet zoveel fout gaan. Als je een patiënt hebt die kritisch is, zoals op ic, die wel zuurstofbehoeftig is en aan allerlei registratieapparatuur hangt voor zijn vitale functies, dan ben je echt super afhankelijk van stroomvoorziening of batterijen en accu's. Daarnaast ben je ook afhankelijk van je patiënten informatiesysteem.''*

Jeroen Geerdink van Ziekenhuisgroep Twente geeft de volgende voorbeelden over hoe smartapparatuur het diagnostische proces kan beïnvloeden:

- Bij meetapparatuur kan het leiden tot data integrity failure wat kan leiden tot foute meetwaarden. Op basis van deze foute meetwaarden wordt er verkeerd patiëntbeleid gevoerd, wat resulteert in schade bij de patiënt.
- Bij een infusiepomp kunnen de instellingen van de pomp remote worden gewijzigd waardoor de dosering foutief is, wat weer kan resulteren in schade bij de patiënt (Geerdink, 2017).

Er zijn veel soorten beveiligingsincidenten die kunnen plaatsvinden. De instellingen van smartapparatuur kunnen worden veranderd. Vervolgens worden organisaties afgeperst voor geld (Santos, 2015). Volgens Santos kunnen er op smartapparatuur zogeheten 'Trojaanse paarden' worden geïnstalleerd om te spioneren. Daarnaast kunnen kwaadwillenden de controle over het apparaat overnemen.

De impact van een aanval kan hoog zijn, met name de kosten die daarbij komen kijken. De kosten variëren van herstellen van beschadigde systemen, gestolen geld, financiële compensatie voor benadeelden, boetes en juridische kosten (Van Rijsewijk, 2016). Volgens van Rijsewijk hebben immateriële kosten nog meer impact. Het gaat hier om het verlies van vertrouwen in de organisatie, verlies van data en reputatieschade.

4.2.4.1 Kritische processen

Volgens Wijn (2017) lopen kritische processen van ziekenhuizen en individuele zorginstellingen risico bij het gebruik van smartapparatuur in het bedrijfsnetwerk. De kritische processen zijn volgens Wijn de processen waarbij de zorgcontinuïteit of patiëntveiligheid niet voldoende wordt geborgd. Alle processen en voorzieningen zijn volgens Wijn weer anders per afdeling. Wijn (2017) zegt over de kritische processen: *''ICT is een belangrijke voorziening. Dat is het proces waarmee je alle patiëntgegevens registreert. Alle onderzoeksresultaten en dergelijke. Als dat uitvalt dan heb je een probleem. We zijn geheel digitaal en er zijn eigenlijk geen papieren dossiers. Er zijn wel back-up stations in huis maar die zitten zo maximaal mogelijk uit elkaar. Als dat uitvalt dan heb je daadwerkelijk wel een probleem voor de zorgcontinuïteit, want daar staat ook bijvoorbeeld medicatie in genoteerd en diëten staan erin genoteerd.*" Wijn vindt net als de andere experts de patiëntdata het belangrijkste proces binnen een organisatie. Daar horen ook het apothekers- en voedingssysteem bij. Deze digitale systemen zijn allemaal digitaal geregeld en zijn daardoor kwetsbaar voor kwaadwillenden en cyberaanvallen. De gevolgen van het ontregelen van deze systemen zijn het leveren van verkeerde zorg. Dit komt doordat de gegevens van patiënten niet meer beschikbaar zijn.

Volgens Wijn (2017) zijn bij het verlenen van deze zorg bepaalde voorzieningen nodig die het primaire zorgproces ondersteunen. Patiënt zijn afhankelijker van het ene proces dan van het andere. Water en stroom hebben direct invloed op de patiëntveiligheid of zorgcontinuïteit, maar gas heeft dat minder. Dit komt doordat de patiënten wel zonder verwarming kunnen. Gea Wijn geeft aan dat er in het Deventer Ziekenhuis continuïteitsplannen voor aanwezig zijn. Er zijn plannen, waarin staat hoe een verpleegkundige moet handelen wanneer zelfs back-up voorzieningen niet meer werken. De technische dienst heeft al veel noodvoorzieningen geregeld, waardoor de dienstdoende verpleegkundige er niets van hoeft te merken.

4.2.5 Risicobewustzijn

Nu duidelijk is welke risico's er spelen en wat de mogelijke impact hiervan is, is het belangrijk om te weten of organisaties zich bewust zijn van deze risico's. Het risicobewustzijn geeft inzicht in hoe de medewerkers nu met smartapparatuur omgaan en hoe erover de risico's wordt gedacht. Volgens Huinink (2017) is bij het Medisch Spectrum Twente de Information Security Officer kenbaar met de risico's van smartapparatuur en zijn de medewerkers zich minder bewust van de cyberrisico's. Dit komt, volgens Huinink, doordat de medewerkers weten dat er iets kan gebeuren, maar niet weten dat het in een ziekenhuis kan gebeuren. Volgens Van Rijsewijk is het naïef om te denken dat kwaadwillenden alleen maar aanvallen uitvoeren in sectoren waar veel geld te halen is, zoals bij banken. Eke organisatie heeft waardevolle zaken voor een kwaadwillende. Vaak worden organisaties volledig willekeurig uitgekozen door geautomatiseerde technologie. Deze zoekt naar kwetsbaarheden en die worden dan misbruikt. Bij het St. Jansdal ziekenhuis is er wel zicht op standaard risico's die voor de hand liggen. Bij Ziekenhuisgroep Twente worden er al risicoanalyses uitgevoerd, wat betekent dat ze er al wel bewust van zijn. Volgens Stoelinga (2017) zijn organisaties zich onvoldoende bewust van de risico's van smartapparatuur, omdat de medewerkers het er nooit over hebben. Wijn, geeft aan dat de medewerkers van het Deventer Ziekenhuis, worden geschoold in kritische processen en patiëntveiligheid. Dit betekent dat de medewerkers daar bewust van worden gemaakt.

4.2.6 Risicoanalyse

De koepelmethodiek is uitgevoerd met behulp van deskresearch, interviews en eigen inzichten. De koepelmethodiek is uitgewerkt in onderstaande tabellen.

Koepelmethodiek
Vragen over Vitale belangen en Systemen
Wat zijn vitale producten en diensten? Het leveren van Zorg (preventieve, acute, chronische, urgente, electieve, …) (Bureau HHM, 2011).
Welke situaties proberen we te voorkomen? Kritische processen worden beïnvloed doordat kwaadwillenden hierbij kunnen, via smartapparatuur en het interne netwerk. Wanneer dit gebeurt, kan de patiëntveiligheid in gevaar komen en kan er geen goede zorg meer worden geleverd. Het gevolg hiervan kan in ziekenhuizen leiden tot slachtoffers en in individuele zorginstellingen tot het leveren van verkeerde zorg.
Hoe zien de sector en de relevante omgeving eruit? Er zijn 211.110 overheid- en zorginstellingen en 261 verplegings- en zorginstellingen met overnachtingen. Volgens de BSI 2008: Gezondheids- en welzijnszorg: Gezondheidszorg, verpleging, verzorging en begeleiding met overnachting en maatschappelijke dienstverlening zonder overnachting (CBS, 2016). De zorgsector wordt onderzocht door te kijken naar ziekenhuizen en individuele zorginstellingen.
Wat zijn de relevante processen en systemen bij de totstandkoming van die producten en diensten? • Primaire processen in het ziekenhuis volgens bureau HHM: leveren van zorg: vaststellen van zorgbehoefte→diagnosticeren→opstellen behandelplan→behandelen→overdragen. • Ondersteunende processen: beheren gebouw, inkoop, HRM, financiële administratie, juridische ondersteuning, ICT-diensten, communicatie en voorlichting, medische technologie, hoteldiensten, veiligheid-, kwaliteit-, arbo- en milieudiensten (Bureau HHM, 2011). • Primair proces individuele zorginstellingen volgens Ziraonline: cliënt met verblijfsindicatie in ZZP→cliënt in zorg bij zorgaanbieder→cliënt uit zorg→exitgesprek oftewel: intake→ zorgplanning→zorgverlening→evaluatie.

• *Belangrijke systemen:* intake→cliëntdossier, zorgovereenkomst, zorgplan, productenboek zorgverlening→cliëntdossier, zorgplan evaluatie→zorgovereenkomst, zorgplan, registratiegegevens. • Secundaire processen: communicatie cliënt, personeelsplanning, zorginkoop/financiën, interne budgettering (Ziraonline, 2016).
Welke partijen zijn verantwoordelijk voor deze processen, systemen en knooppunten? ICT en Technische Dienst spelen een grote rol, maar de raad van bestuur is eindverantwoordelijk.
Welke externe ontwikkelingen leiden mogelijk tot kwetsbaarheden? De ontwikkeling van de vaardigheden en expertise van hackers. De digitale ontwikkeling van de samenleving brengt kwetsbaarheden met zich mee. Wanneer alles aan het internet wordt gekoppeld, is het kwetsbaarder voor cyberaanvallen.
Welke bestaande maatregelen zijn al genomen? • Risicoanalyse bij aanschaf smartapparatuur. • Impact van het apparaat wordt bepaald.
Welke maatregelen kunnen op draagvlak rekenen en welke niet? De maatregelen die betrekking hebben op het gebruik en de aanschaf van de apparaten kunnen worden uitgevoerd. Die maatregelen die betrekking hebben op de producent kunnen niet op veel draagvlak rekenen.

Tabel 2 Vragen over vitale belangen en systemen

Vragen over beoordeling en prioritering van impact	
Wat zijn de meest relevante kans-effect-combinaties	Zie Kans-effect matrix in ***paragraaf 4.2.6.2***
Wat voor (typen) effecten kunnen zich voordoen?	• Financiële schade • Imago Schade • Onderbreken van zorgproces met dodelijke gevolgen

Tabel 3 Vragen over beoordeling en prioritering van impact

Vragen over identificatie van dreigingen	
Welke (typen) dreigingen kunnen zich (in de toekomst) voordoen?	Zie pad analyse in ***paragraaf 4.2.6.1***

Tabel 4 Vragen over identificatie van dreigingen

Vragen over de formulering, beoordeling en implementatie van maatregelen
Welke typen maatregelen zijn te onderscheiden? <u>Aanschaf van smartapparatuur:</u> • Koop alleen apparaten van producenten waarvan bekend is dat de producten veilig zijn (FBI, 2015). • Ga op onderzoek uit op het internet voordat een apparaat wordt aangeschaft. Het kan zijn dat deze al is onderzocht door veiligheidsonderzoekers, die de zwakke apparaten eruit halen (Kaspersky, 2015). • Koop smartapparatuur die al wat langer op de markt is en wees voorzichtig met nieuwe producten. Deze kunnen naast bugs en softwareproblemen ook beveiligingsproblemen bevatten die nog niet zijn ontdekt door veiligheidsonderzoekers (Kaspersky, 2015). • Kies verstandig welk smartapparaat wel of niet in de organisatie kan worden gebruikt, rekening houdend met de veiligheidsrisico's (Kaspersky, 2015). • Zoek naar standaardisatie. Dit is nog in een vroeg stadium maar binnenkort zullen er standaarden verschijnen voor smartapparatuur, inclusief veiligheidsnormen (Santos, 2015).

Gebruik van Smartapparatuur

- Alle persoonlijke apparaten moeten worden geïntegreerd in een securitystrategie. Het is cruciaal om in kaart te brengen welke apparaten data uitwisselen met het bedrijfsnetwerk. Zo kan er een gedegen securitystrategie worden bepaald (Lacroix, 2017).
- De apparaten moeten altijd worden geüpdatet met de laatste beveiligingspatches (FBI, 2015). Deze beveilgingspatches zullen het apparaat beschermen tegen aanvallen.
- Verander het standaardwachtwoord. Stel een pincode of een sterk, uniek wachtwoord in (FBI, 2015).
- Sluit smartapparatuur op het gastnetwerk van de router aan, zodat kwaadwillenden niet bij vitale onderdelen van het netwerk kunnen (Hellodigital, 2017).
- Pas op met smartapparatuur die constant met internet in verbinding staat wanneer deze functie niet door de gebruiker wordt gebruikt. Het is dan veiliger om een normaal apparaat te gebruiken (Hellodigital, 2017).
- Check de wifidekking waar de smartapparatuur aan wordt gehangen. Zorg dat deze sterk en betrouwbaar is (Hellodigital, 2017).
- Check of het apparaat zonder internet werkt, zodat de gebruiker het nog steeds kan gebruiken wanneer het internet niet meer functioneert (Hellodigital, 2017).
- Implementeer de smartapparatuur in de business continuity plannen of crisisplannen (Santos, 2015).
- Beheer wie gebruik maakt van de smartapparatuur, ontwikkel beleid en maak duidelijk wie toegang heeft tot de apparatuur (Santos, 2015).
- Zorg niet alleen voor goede informatiebeveiliging met firewalls, maar zorg ook voor inbraakpreventie (Santos, 2015).
- Geef de medewerkers meer verantwoordelijkheid qua gebruik. Hierdoor wordt er verantwoorder met de apparatuur omgegaan (Van Rijsewijk, 2016).
- Stuur op vertrouwen en geef medewerkers meer beslissingsruimte (Van Rijsewijk, 2016).

Privacy

- Lees de privacy voorwaarden. De fabrikant kan gegevens over de gebruiker verzamelen. Wanneer deze onduidelijk zijn, is het verstandiger om er geen gebruik van te maken (Chapin, Eldridge, & Rose, 2015).

Producent

- Bij het ontwerp moet er een plan zijn voor de beveiliging (Domotica, 2017).
- Investeren in beveiliging in de ontwerpfase is vaak veel goedkoper dan wanneer je achteraf beveiliging moet toevoegen (Domotica, 2017).
- In het ontwerpproces moeten de smartapparaten als kleine computers worden beschouwd. De producent moet zich goed beseffen wat interessant is voor kwaadwillenden (Domotica, 2017).
- Bedenk goed wat er gebeurt met de apparatuur wanneer deze de houdbaarheidsdatum heeft bereikt. Slechts een mail sturen, met de melding dat het apparaat niet meer wordt ondersteund is niet voldoende (Domotica, 2017).

Tabel 5 Vragen over de formulering, beoordeling en implementatie van maatregelen

4.2.6.1 Pad analyse

De pad analyse is een methode afkomstig uit de koepelmethodiek waarmee dreigingen in kaart kunnen worden gebracht. Deze dreigingen kiezen het pad van de minste weerstand. Het is de bedoeling dat deze scenario's (paden) worden uitgeschreven, zodat de paden met de minste weerstand zichtbaar worden. Pad 1 is het pad met de minste weerstand, gevolgd door pad 2 en pad 3. De dreigingen zijn kwaadwillenden afkomstig uit het Cybersecuritybeeld Nederland 2016 (Nationaal Cyber Security Centrum, 2016).

Ziekenhuis	
Beroepscrimineel	
Pad 1	Afpersen van medewerkers door bijvoorbeeld ransomware, malware, cryptoware te versturen of een DDoS-aanval uit te voeren via de minst beveiligde apparatuur, die in verbinding staan met het interne netwerk zoals smartapparatuur.
Pad 2	Afpersen van medewerkers door bijvoorbeeld ransomware, malware, cryptoware te versturen of een DDoS-aanval uit te voeren via computersystemen.
Pad 3	Afpersen van medewerkers door het hacken van openstaande computers waar je fysiek zo bij kan. Voorbeelden hiervan zijn: het inpluggen van een USB-stick of het vinden van wachtwoorden genoteerd op papier.
Terrorist	
Pad 1	Het ziekenhuis is een openbare ruimte, dus wanneer de terrorist het pad van de minste weerstand wil nemen dan loopt deze naar binnen zonder tegen gehouden te worden. Eenmaal binnen kan de terrorist met wapens schade aanrichten. Er is wel beveiliging aanwezig, maar deze zal niet opgewassen zijn tegen gewapende terroristen.
Pad 2	Een aanval uitvoeren van buiten het pand door bijvoorbeeld bommen te plaatsen of door het rammen van het gebouw met een vrachtwagen.
Pad 3	Een cyberaanval op het ziekenhuis uitvoeren waarbij het zorgproces wordt onderbroken en er geen goede zorg meer kan worden geleverd. Dit kan dodelijke gevolgen hebben.
Cybervandalen en scriptkiddies	
Pad 1	Verstoring van de ICT door een DDoS-aanval uit te voeren uit baldadigheid, voor de uitdaging of om de eigen capaciteit aan te tonen. Vaak hebben ze weinig kennis en voeren ze alleen een aanval uit die makkelijk uit te voeren is.
Pad 2	Diefstal van computergegevens zal in mindere mate voorkomen en is niet heel waarschijnlijk.
Interne Actoren	
Pad 1	Het lekken van data door onzorgvuldigheid en onbewustheid van een medewerker. De medewerker is zich er niet van bewust data te lekken en doet dit door foutief menselijk handelen. Dit varieert van het kwijtraken van gegevens tot het online beschikbaar maken van gegevens.
Pad 2	Er zijn ook interne actoren die moedwillig systemen willen manipuleren of gegevens willen lekken. Deze acties worden uitgevoerd uit financiële, politieke en persoonlijke redenen.
Pad 3	Interne actoren richten fysieke schade aan op bepaalde personen of systemen.

Tabel 6 Pad Analyse Ziekenhuis

Individuele zorginstelling	
Beroepscrimineel	
Pad 1	Afpersen van medewerkers door bijvoorbeeld ransomware, malware, cryptoware te versturen of een DDoS-aanval uit te voeren via de minst beveiligde apparatuur die in verbinding staan met het interne netwerk zoals smartapparatuur.
Pad 2	Afpersen van medewerkers door bijvoorbeeld ransomware, malware, cryptoware te versturen of een DDoS-aanval uit te voeren via computersystemen
Pad 3	Afpersen van medewerkers door het hacken van openstaande computers waar je fysiek zo bij kan. Voorbeelden hiervan zijn: het inpluggen van een USB-stick of het vinden van wachtwoorden genoteerd op papier.
Cybervandalen en scriptkiddies	
Pad 1	Verstoring van de ICT door een DDoS-aanval uit te voeren uit baldadigheid, voor de uitdaging of om de eigen capaciteit aan te tonen. Vaak hebben ze weinig kennis en voeren ze alleen een aanval uit die makkelijk uit te voeren is.

Pad 2	Diefstal van computergegevens zal in mindere mate voorkomen maar is niet heel waarschijnlijk.
Interne Actoren	
Pad 1	Het lekken van data door onzorgvuldigheid en onbewustheid van een medewerker. De medewerker is zich er niet van bewust data te lekken en doet dit door foutief menselijk handelen. Dit varieert van het kwijtraken van gegevens tot het online beschikbaar maken van gegevens.
Pad 2	Er zijn ook interne actoren die moedwillig systemen willen manipuleren of gegevens willen lekken. Deze acties worden uitgevoerd uit financiële, politieke en persoonlijke redenen.
Pad 3	Interne actoren richten fysieke schade aan op bepaalde personen of systemen.
Private organisaties	
Pad 1	Vertrouwelijkheid van systemen aantasten voor financieel gewin of digitale aanvallen uitvoeren om de concurrentiepositie te verbeteren. Het hacken van deze systemen gebeurt via de systemen met de minste weerstand. Dit zal goed kunnen via smartapparatuur, omdat deze nog niet optimaal beveiligd zijn.
Pad 2	Vertrouwelijkheid van systemen aantasten voor financieel gewin of digitale aanvallen uitvoeren om de concurrentiepositie te verbeteren. Wanneer smartapparatuur beter beveiligd is dan zullen de hackers het via computersystemen proberen.

Tabel 7 Pad Analyse Individuele zorginstelling

Uit de pad analyse komt naar voren dat beroepscriminelen de grootste dreiging zijn voor ziekenhuizen en individuele zorginstellingen. Doordat smartapparaten nu het kwetsbaarst zijn, is het waarschijnlijk dat het er via smartapparatuur een aanval wordt uitgevoerd. Daarnaast is het goed mogelijk dat interne actoren onzorgvuldig zijn en onbewust data lekken. Bij het gebruik van smartapparatuur vergroot de dreiging van de kwaadwillenden. Deze zoeken de weg met de minste weerstand, op dit moment is dit voor beroepscriminelen en private organisaties het geval.

4.2.6.2 Kans-effect matrix

Hieronder is de kans-effect matrix uitgewerkt. Dit model is afkomstig uit de koepelmethodiek. Allereerst worden er gebeurtenissen geschetst, vervolgens worden deze in de kans-effect matrix geplaatst. Op de verticale as staan de kansen en op de horizontale as staan de effecten. Uiteindelijk wordt bepaald hoe kritisch deze gebeurtenis is.

- Gebeurtenis 1(G1): een kwaadwillende kan via smartapparatuur patiëntgegevens veranderen, waardoor er verkeerde zorg wordt geleverd. Dit kan in het ergste geval leiden tot dodelijke slachtoffers.
- Gebeurtenis 2(G2): een kwaadwillende kan via smartapparatuur patiëntgegevens verwijderen, waardoor er geen zorg kan worden verleend. Dit kan in het ergste geval leiden tot dodelijke slachtoffers.
- Gebeurtenis 3(G3): een smartapparaat wordt overgenomen door een kwaadwillende, waardoor deze op een verkeerde manier wordt gebruikt.
- Gebeurtenis 4 (G4) een smartapparaat wordt uitgeschakeld door een kwaadwillende.
- Gebeurtenis 5(G5): een kwaadwillende kan via smartapparatuur bij vitale systemen komen en legt deze plat.

Zeer Waarschijnlijk					
Waarschijnlijk					
Mogelijk		G3, G4			G1, G2, G5
Onwaarschijnlijk					
Zeer onwaarschijnlijk					
	Onbelangrijk	Weinig	Gemiddeld	Veel	Catastrofaal

Tabel 8 Kans-effect matrix

Kritisch?	
	Hoog
	Significant
	Gemiddeld
	Laag

Tabel 9 Kritische niveaus

Er moet worden gezorgd dat kwaadwillenden niet bij de patiëntgegevens en vitale systemen kunnen komen, aangezien de gevolgen catastrofaal zijn. Het kritische niveau van deze gebeurtenissen is hoog. Het is mogelijk dat het voorkomt dus er moet aandacht aan worden geschonken. Aan het feit dat kwaadwillenden smartapparatuur kunnen overnemen of kunnen uitschakelen moet ook aandacht aan worden geschonken, maar de impact is een stuk minder groot waardoor het minder prioriteit heeft. Het kritische niveau is gemiddeld. Nu de risico's in kaart zijn gebracht, wordt er in de volgende paragraaf uiteengezet welke onderdelen er in het adviesproduct moeten komen, zodat Sincerus een passend advies kan geven over het gebruik van smartapparatuur in de zorgsector.

4.3 Waar moet een adviesproduct aan voldoen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector?

In dit hoofdstuk wordt uiteengezet wat er allemaal in het adviesproduct moet komen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector. Uit een gesprek met de opdrachtgever Sincerus is naar voren gekomen dat het een adviesproduct betreft die wordt gebruikt in de voorfase van het adviesproces. Met dit product moeten potentiële klanten worden binnengehaald. Het is de wens van Sincerus dat het een product betreft die schematisch weergeeft wat een organisatie in de zorgsector kan doen om zich te wapenen tegen risico's van smartapparatuur. In het adviesproduct moeten dus de risico's samen met de maatregelen worden verwerkt. Naast deze aspecten moet ook duidelijk worden gemaakt wat smartapparatuur is. De definitie van smartapparatuur luidt: 'Smartapparaten zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kan zijn op een intern netwerk en met elkaar kunnen communiceren.' Deze definitie moet in het product terug te vinden zijn. Daarnaast worden ook de kwaadwillenden, die een dreiging vormen, in het adviesproduct verwerkt. Uiteindelijk is het de bedoeling dat dit product een checklist wordt, die later ook toegepast kan worden in andere sectoren. Uit een gesprek met Sincerus is ook gebleken dat er nog geen vaste formats zijn wat betreft advies. Er zijn dus nog geen standaardvoorwaarden waar het adviesproduct aan moet voldoen. De risico's die in het product weergegeven moeten worden zijn uiteengezet in het vorige resultatenhoofdstuk. De maatregelen die in het product worden gebruikt worden hieronder weergegeven. Deze resultaten zijn behaald door middel van interviews met experts en door het uitvoeren van een risicoanalyse.

4.3.1 Maatregelen

Volgens expert Stoelinga zijn er verschillende categorieën in de maatregelen te onderscheiden. Organisatorische maatregelen, technische maatregelen en psychologische maatregelen (Stoelinga, 2017). Geerdink (2017) van Ziekenhuisgroep Twente geeft ook aan dat er technische en organisatorische maatregelen moeten worden toegepast conform de richtlijnen NEN 7510/12/13.
Volgens Stoelinga zijn de maatregelen die getroffen moeten worden hetzelfde als bij niet-smartapparatuur, met uitzondering van de technische maatregelen. De technische maatregelen zijn belangrijk, maar dit geldt ook voor de organisatorische maatregelen. Technische maatregelen zoals wachtwoordmanagement en organisatorische maatregelen zoals acces control zijn hier voorbeelden van. Stoelinga (2017): ''*Het is belangrijk dat het risicomanagementcyclus goed is ingebed in het bedrijfsproces,*

dat daar op gemonitord wordt en jaarlijks gereviewd wordt.'' Om ervoor te zorgen dat kritische processen geen gevaar lopen bij het gebruik van smartapparatuur, is het volgens Stoelinga eerst belangrijk dat er één iemand verantwoordelijk wordt gesteld voor de security in ziekenhuizen. Stoelinga (2017) geeft aan: *''Dingen die in de industrie volstrekt normaal zijn, vind ik bij ziekenhuizen altijd tegenvallen. Ik heb geen harde cijfers, maar ik denk dat er nog wel ruimte voor verbetering in zit.''* Volgens Stoelinga kan een maatregel tegen de gebruiksrisico's, awareness training met co-creatie zijn. De werkvloer moet bij het proces worden betrokken. Het werkt niet als er alleen wordt gezonden. Betrek alle stakeholders bij het probleem. Zo creëer je meer draagvlak voor het uitvoeren van bepaalde regels.

- Schat de risico's in op impact en likelyhood
- Maak geen gebruik van smartapparatuur in de organisatie

Stoelinga (2017) zegt het volgende over of het verstandig is voor ziekenhuizen om smartapparatuur nu te gebruiken, nu het nog niet goed beveiligd is: *''Ik zal die apparatuur alleen maar nemen als het wel goed beveiligd is. Het is sowieso een goed idee om het hele ziekenhuis te beveiligen.''* Stoelinga vindt dat de organisaties nog een hele slag moeten slaan. Om ervoor te zorgen dat de belangrijke kritische processen in de organisatie geen gevaar lopen, moet een organisatie volgens Wijn (2017) de volgende maatregelen treffen:

- Breng de kritische processen in kaart
- Maak back-ups van voorzieningen, zodat deze processen nog werken
- Maak beheersplannen voor wanneer een kritisch proces uitvalt
- Ontwikkel protocollen

Uit de risicoanalyse zijn de volgende maatregelen naar voren gekomen die gebruikt kunnen worden in het adviesproduct:

- Koop alleen apparaten van producenten waarvan bekend is dat de producten veilig zijn (FBI, 2015).
- Ga op onderzoek uit op het internet voordat een apparaat wordt aangeschaft. Het kan zijn dat deze al is onderzocht door veiligheidsonderzoekers, die de zwakke apparaten eruit halen (Kaspersky, 2015).
- Koop smartapparatuur die al wat langer op de markt is en wees voorzichtig met nieuwe producten. Deze kunnen naast bugs en softwareproblemen ook beveiligingsproblemen bevatten die nog niet zijn ontdekt door veiligheidsonderzoekers (Kaspersky, 2015).
- Kies verstandig welk smartapparaat wel of niet in de organisatie kan worden gebruikt, rekening houdend met de veiligheidsrisico's (Kaspersky, 2015).
- Zoek naar standaardisatie. Dit is nog in een vroeg stadium maar binnenkort zullen er standaarden verschijnen voor smartapparatuur, inclusief veiligheidsnormen (Santos, 2015).
- Alle persoonlijke apparaten moeten worden geïntegreerd in een securitystrategie. Het is cruciaal om in kaart te brengen welke apparaten data uitwisselen met het bedrijfsnetwerk. Zo kan er een gedegen securitystrategie worden bepaald (Lacroix, 2017).
- De apparaten moeten altijd worden geüpdatet met de laatste beveiligingspatches (FBI, 2015). Deze beveilgingspatches zullen het apparaat beschermen tegen aanvallen.
- Verander het standaardwachtwoord. Stel een pincode of een sterk, uniek wachtwoord in (FBI, 2015).
- Sluit smartapparatuur op het gastnetwerk van de router aan, zodat kwaadwillenden niet bij vitale onderdelen van het netwerk kunnen (Hellodigital, 2017).

- Pas op met smartapparatuur die constant met internet in verbinding staat wanneer deze functie niet door de gebruiker wordt gebruikt. Het is dan veiliger om een normaal apparaat te gebruiken (Hellodigital, 2017).
- Check de wifidekking waar de smartapparatuur aan wordt gehangen. Zorg dat deze sterk en betrouwbaar is (Hellodigital, 2017).
- Check of het apparaat zonder internet werkt, zodat de gebruiker het nog steeds kan gebruiken wanneer het internet niet meer functioneert (Hellodigital, 2017).
- Implementeer de smartapparatuur in de business continuity plannen of crisisplannen (Santos, 2015).
- Beheer wie gebruik maakt van de smartapparatuur, ontwikkel beleid en maak duidelijk wie toegang heeft tot de apparatuur (Santos, 2015).
- Zorg niet alleen voor goede informatiebeveiliging met firewalls, maar zorg ook voor inbraakpreventie (Santos, 2015).
- Geef de medewerkers meer verantwoordelijkheid qua gebruik. Hierdoor wordt er verantwoorder met de apparatuur omgegaan (Van Rijsewijk, 2016).
- Stuur op vertrouwen en geef medewerkers meer beslissingsruimte (Van Rijsewijk, 2016).
- Lees de privacy voorwaarden. De fabrikant kan gegevens over de gebruiker verzamelen. Wanneer deze onduidelijk zijn, is het verstandiger om er geen gebruik van te maken (Chapin, Eldridge, & Rose, 2015).

Wanneer de belangrijkste risico's samen met de maatregelen worden verwerkt in het adviesproduct, is het voor Sincerus mogelijk om een passend advies te geven over wat organisaties kunnen doen wanneer er gebruikt wordt gemaakt van smartapparatuur in het bedrijfsnetwerk.

5. Conclusie

Met dit onderzoek is getracht een antwoord te vinden op de vraag: '*Welke risico's spelen er in de zorgsector bij het gebruik van smartapparatuur in het bedrijfsnetwerk, hoe zijn deze eventuele risico's inzichtelijk te maken en welke maatregelen kunnen er getroffen worden om eventuele risico's te voorkomen?*' Aan de hand van dit onderzoek zijn de volgende conclusies getrokken:

In welke mate speelt smartapparatuur een rol in de zorgsector?
Uit onderzoek is gebleken dat smartapparatuur een rol speelt binnen de zorgsector en die zal alleen maar groter worden. De onderzochte organisaties in de zorgsector zijn bekend met smartapparatuur en hebben deze al geïmplementeerd. Hoewel de organisaties de apparatuur reeds geïmplementeerd hebben, ontbreekt er enige kennis wat betreft de apparatuur. Er valt te concluderen dat ziekenhuizen meer smartapparatuur gebruiken dan een individuele zorginstelling. Dit komt onder andere doordat ziekenhuizen gebruik maken van smart health en een individuele zorginstelling over het algemeen niet. De zorgsector is één van de meest geavanceerde sectoren in het implementeren van IoT-toepassingen. Er wordt door ruim 60% van alle zorgorganisaties wereldwijd gebruik gemaakt van IoT-toepassingen, waar smartapparatuur onderdeel van uit maakt. Er wordt het meest gebruik gemaakt van smart-tv's, smartwatches en smart health.

Welke risico's zijn er aanwezig bij het gebruik van smartapparatuur in het bedrijfsnetwerk en in welke mate zijn organisaties zich bewust van deze risico's?
Wanneer een organisatie in de zorgsector smartapparatuur wil gebruiken in het bedrijfsnetwerk, dan moet er rekening worden gehouden met diverse risico's. Deze zijn onderverdeeld in technische risico's, privacy risico's en gebruiksrisico's. De belangrijkste technische risico's zijn: het beveiligingsniveau; de implementatie van de beveiliging in het productieproces; de apparaten zijn niet of nauwelijks te updaten; de lange levensduur van de apparaten, waardoor de ondersteuning van de producent in gevaar komt. De belangrijkste privacy risico's zijn: apparaten kijken en luisteren mee; geen gebruikersinterface om privacy voorwaarden te accepteren; gebruiker heeft geen zicht op de gegevens die worden verwerkt en gebruik in de privésfeer wekt andere privacy verwachtingen. De belangrijkste gebruiksrisico's zijn: medewerkers zijn niet bereid veel wachtwoorden in te voeren, standaardwachtwoorden worden niet veranderd; medewerkers denken dat andere organisaties eerder worden getroffen dan de eigen organisatie; medewerkers zijn minder bereid om regels na te leven; security wordt omzeild uit gemak; informatiebeveiliging heeft geen prioriteit en social engineering. Sommige medewerkers in de zorgorganisaties zijn zich bewust van de risico's, maar over het algemeen wordt er binnen de organisaties niet over gesproken.

Waar moet een adviesproduct aan voldoen om advies te kunnen geven over het gebruik van smartapparatuur in de zorgsector?
Het adviesproduct moet een product zijn waarmee Sincerus potentiële klanten kan werven. Bij het eerste gesprek wordt met behulp van een checklist advies gegeven over het gebruik van smartapparatuur. Op deze manier moet de klant gestimuleerd worden om de informatiebeveiliging te optimaliseren met behulp van Sincerus. Het is van belang dat de risico's en de maatregelen worden benoemd. De maatregelen die een organisatie kan treffen zijn hetzelfde als bij de algemene informatiebeveiliging: breng de kritische processen in kaart; maak back-ups van voorzieningen, zodat deze processen nog werken; maak beheersplannen voor wanneer een kritisch proces uitvalt en ontwikkel protocollen. Andere belangrijke maatregelen specifiek voor smartapparatuur zijn: zorg ervoor dat de smartapparatuur niet aan kritische processen wordt gekoppeld, maar bij voorkeur aan het gastnetwerk; gebruik de smartapparatuur alleen wanneer het nodig is gezien de kwetsbaarheid. Naast deze maatregelen moet het begrip smartapparatuur worden uitgelegd en moeten de dreigingen worden benoemd. Al deze componenten vormen de basis voor een gedegen adviesproduct, waarmee advies gegeven kan worden over het gebruik van smartapparatuur in de zorgsector.

6. Aanbevelingen

In dit hoofdstuk worden de aanbevelingen weergegeven die voortvloeien uit de conclusie.

Test smartapparatuur

Uit het onderzoek is gebleken dat de beveiliging van smartapparatuur nog op een laag niveau is. Hier kan Sincerus op inspelen door smartapparatuur te testen. De grootste winst is niet te halen bij de organisaties, maar bij de producenten. De beveiliging van smartapparatuur is in de meeste gevallen in de designfase niet goed genoeg. Het wordt niet goed toegepast of het wordt helemaal niet toegepast. Het grootste risico is dus niet hoe de gebruikers met het product omgaan, maar hoe het apparaat wordt ontworpen. Wanneer Sincerus bepaalde smartapparatuur test en daarmee kwetsbaarheden blootlegt, kan Sincerus mogelijk meer naamsbekendheid genereren, wat leidt tot meer klanten.

Keurmerk smartapparatuur

Naast het testen van smartapparatuur kan het een goed idee zijn om als Sincerus een eigen keurmerk te ontwikkelen. Dit keurmerk geeft aan of smartapparatuur veilig is voor gebruik. Naast dit keurmerk kan Sincerus de klant helpen met het aanschaffen van veilige smartapparatuur binnen de organisatie. Zo biedt Sincerus een extra service aan de klant, die voorheen nog niet werd aangeboden.

Adviesproduct

Uit het onderzoek is gebleken dat het adviesproduct een checklist moet zijn. In deze checklist moeten onder andere de risico's en maatregelen die bij het gebruik van smartapparatuur in het bedrijfsnetwerk spelen worden benoemd. Dit onderzoek is uitgevoerd in de zorgsector maar het adviesproduct kan op bijna alle andere sectoren worden toegepast. De risico's en maatregelen zullen aardig overeenkomen bij andere sectoren.

Formats voor advies

In dit onderzoek is naar voren gekomen dat er bij Sincerus geen formats worden gehanteerd voor het geven van advies. Het is dus mogelijk om in dit aspect de organisatie te verbeteren. Het advies is per organisatie nooit hetzelfde, maar zal vaak overeenkomsten vertonen. Er kan op een heleboel punten dus standaard hetzelfde advies worden gegeven. De kwaliteit van het advies zal een stuk beter zijn, aangezien het altijd aan de standaard eisen voldoet. Uiteindelijk scheelt dit ook tijd.

Aanvullend onderzoek

In dit onderzoek is er onderzocht wat de rol van smartapparatuur binnen de zorgsector is. Wegens tijdsbestek zijn er vier zorgorganisaties voor dit onderzoek onderzocht. Wanneer er een compleet beeld moet worden geschetst van een gehele sector, is het wenselijk om meerdere organisaties te benaderen. Het onderzoek kan dan een kwantitatief onderzoek zijn, dat uitgevoerd kan worden met behulp van enquêtes.

7. Discussie

In dit hoofdstuk worden de beperkingen en de bijzonderheden van de methodes, resultaten en conclusies weergegeven.

Methode van onderzoek

Interviews

Het was de bedoeling dat er vijf organisaties werden onderzocht om zo een representatief beeld te schetsen van de zorgsector. Van drie ziekenhuizen en twee andere zorgorganisaties moest een medewerker worden geïnterviewd die verstand heeft van de smartapparatuur binnen de organisatie. Uiteindelijk zijn het er vier geworden, waarvan drie ziekenhuismedewerkers en één medewerker van een individuele zorginstelling. Helaas konden veel organisaties geen tijd of ruimte vinden om mee te werken aan dit afstudeeronderzoek. Er zijn veel zorgorganisaties telefonisch benaderd, waar vervolgens op gereageerd werd met: *''Stuur maar een mail.''* Na het verzenden van deze mail, werd er nooit op geantwoord. Een aantal organisaties gaven in eerste instantie aan mee te willen werken, maar uiteindelijke bleek dit toch niet te lukken. Zo was er vanuit het Deventer Ziekenhuis een toezegging gedaan, dat er naast Gea Wijn, ook iemand van de ICT beschikbaar zou zijn voor de vragen over smartapparatuur. Dit bleek niet het geval en achteraf wilde de ICT-medewerkers niet meer meewerken wegens tijdgebrek. Dit kan ervoor zorgen dat het onderzoek minder valide is, dan van tevoren werd gedacht. Doordat tijdens het onderzoek interviewgegevens verloren zijn gegaan, kan het zijn dat er een minder betrouwbaar beeld is geschetst dan voorheen werd gedacht. Dit is gecompenseerd door aanvullend literatuuronderzoek en deskresearch.

Koepelmethodiek

Er is ook gebruik gemaakt van de koepelmethodiek om een risicoanalyse uit te voeren. Tijdens het uitvoeren van het onderzoek leek deze methode minder geschikt dan vooraf werd gedacht. Er is hierom gekozen om deze koepelmethodiek voor een gedeelte uit te voeren. Er waren onderdelen bij die niet relevant waren voor dit onderzoek. Wanneer er echt een goede risicoanalyse via de koepelmethodiek gemaakt moet worden, kan dit beter binnen één organisatie worden gedaan. Het kost veel tijd om een risicoanalyse te maken, daarom zou het beter zijn om dit in een apart onderzoek te doen.

Resultaten

De resultaten van dit onderzoek zijn niet geheel opvallend te noemen. Voor het onderzoek werd er door de opdrachtgever al verwacht dat er risico's zouden spelen bij het gebruik van smartapparatuur in de zorgsector. Het was voornamelijk de vraag, welke risico's dat zouden zijn. Het opvallendste resultaat is dat het grootste probleem niet bij de gebruikers van de smartapparatuur ligt, maar bij de producenten van de smartapparaten. De producenten moeten zorgen dat de apparaten betere beveiliging krijgen, zodat de gebruikers daar later weinig omkijken naar hebben. Een ander opvallend resultaat is dat er in de individuele zorginstelling nog bijna geen smartapparatuur wordt gebruikt. Dit onderzoek is geen bewijs dat smartapparatuur een rol speelt in alle organisaties van de zorgsector, omdat er maar vier organisaties zijn onderzocht.

Conclusie

Het is de bedoeling dat Sincerus advies gaat geven over het gebruik van smartapparatuur. Dit advies kan gegeven worden aan de hand van het adviesproduct dat reeds gecreëerd is. Van tevoren was het de bedoeling om te onderzoeken wat de eisen zouden zijn van een standaard adviesproduct van Sincerus. Dit is niet te benoemen, omdat Sincerus dit soort producten niet in huis heeft. Het product hoeft dus niet aan bepaalde kwaliteitsnormen te voldoen. Het hoeft enkel een aantal componenten te bevatten.

Bibliografie

Alles Verbonden. (2017, januari 1). *slimme apparaten*. Opgeroepen op februari 13, 2017, van Alles Verbonden: http://www.allesverbonden.nl/slimme-apparaten/

Aruba Networks. (2017). *IoT Healthcare infographic.* Opgeroepen op Juni 2, 2017, van Arubanetworks: http://www.arubanetworks.com/assets/infographic/Aruba_IoT_Healthcare_Infographic.pdf

Bureau HHM. (2011). *Handreiking Stappenplan zorginstellingen.* Enschede: Bureau HHM. Opgehaald van http://www.invoorzorg.nl/docs/ivz/werkenmetZZPs/stappenplan_zorginstellingen_v5.0.pdf

Business Continuity Institute. (2013). *Good Practice Guideline.* Reading: Business Continuity Institute.

CBS. (2016). *Standaardbedrijfsindeling 2008.* Den Haag: Centraal Bureau voor de Statistiek.

CBS Statline. (2017, januari 18). *Bedrijven ;bedrijfstak.* Opgeroepen op februari 9, 2017, van CBS Statline: http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=81589ned&D1=a&D2=1010&D3=25-40&HDR=G2&STB=T,G1&VW=T

CEN. (2014). *ISO 22301.* Brussel: CEN.

Chapin, L., Eldridge, S., & Rose, K. (2015). *The Internet of Things: An overview.* Geneve : The Internet Society .

Cobb, S. (2016, oktober 24). *10 things to know about the October 21 IoT DDoS attacks*. Opgeroepen op februari 2017, 8, van Welivesecurity: http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

Computable. (2017, Maart 3). *KPN CISO waarschuwt voor risico's IoT en 5G*. Opgeroepen op Juni 11, 2017 , van Computable: https://www.computable.nl/artikel/nieuws/security/5969034/250449/kpn-ciso-waarschuwt-voor-risicos-iot-en-5g.html

Dijkzeul, I. A., Mil, I. B., & Pennen, D. R. (2006). *Zicht op Risico's .* Utrecht: Ministerie van Economische Zaken.

Domotica. (2016, oktober 24). *smart home devices ddos aanval*. Opgeroepen op februari 7, 2017, van domotica.nl: https://domotica.nl/2016/10/24/smart-home-devices-ddos-aanval/

Domotica. (2017, maart 9). *hoe je het internet of things beveiligt in 10 stappen*. Opgehaald van Domotica: http://domotica.nl/2017/03/09/hoe-je-het-internet-of-things-beveiligt-in-10-stappen/

Domotica. (2017, mei 5). *verschillen tussen domotica*. Opgeroepen op februari 7, 2017, van domotica: http://domotica.nl/2017/01/05/verschillen-tussen-domotica/

Drieënhuizen, N. (2017, april 4). Interview Niels Drieënhuizen Lindenhout. (J. Seegers, Interviewer)

Eastern Connecticut State University. (2014, Augustus 1). *SmartDeviceEmailAccesWaiver.* Opgeroepen op februari 16, 2017, van Easternct: http://www.easternct.edu/its/files/2014/08/SmartDeviceEmailAccessWaiver.pdf

FBI. (2015, September 10). *Internet of Things Poses Opportunities for Cyber Crime* . Opgeroepen op Juni 13, 2017, van Internet Crime Complaint Center: https://www.ic3.gov/media/2015/150910.aspx

Geerdink, J. (2017, mei 8). Interview Jeroen Geerdink, Ziekenhuisgroep Twente. (J. Seegers, Interviewer)

GFK. (2016). *Smart Home Monitor 2016.* Amstelveen: GFK.

Hager. (2017). *Internet of Things en Domotica.* 's-Hertogenbosch: Hager. Opgehaald van Hager: http://www.hager.nl/whitepapers

Hellodigital. (2017, maart 3). *zijn slimme apparaten wel veilig*. Opgehaald van hellodigital: https://www.hellodigital.nl/leven-werk/amusement/zijn-slimme-apparaten-wel-veilig/

ISO-IEC. (2012). *ISO-IEC 27032*. Opgeroepen op maart 1, 2017, van ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO-IEC. (2013). *ISO2027001.* Geneve : ISO-IEC.

Kaspersky. (2015, december 5). *overleven in de IoT-wereld risico's smartapparatuur slimme woningen in kaart gebracht*. Opgeroepen op juni 16, 2017, van Kaspersky: https://www.kaspersky.nl/about/press-releases/2015_overleven-in-de-iot-wereld-risico-s-apparatuur-slimme-woningen-in-kaart-gebracht

Knieriem, J. (2016, december 17). *trends informatiebeveiliging 2017*. Opgeroepen op februari 7, 2017, van Emerce: http://www.emerce.nl/opinie/dit-trends-informatiebeveiliging-2017

Kregting, M. (2017, Februari 28). *Aruba zorg scoort hoog met IoT-Toepassingen.* Opgeroepen op Juni 2, 2017, van ICT Health: https://www.icthealth.nl/nieuws/nieuwsitem/article/Aruba-zorg-scoort-hoog-met-IoT-toepassingen.html

Lacroix, P. (2017, Januari 9). *De security risico's van internet of things*. Opgehaald van Blogit: http://www.blogit.nl/security-risicos-iot/

Lectoraat Smart Devices. (2017, januari 1). *smart-devices*. Opgeroepen op februari 15, 2017, van Zuyd: https://www.zuyd.nl/onderzoek/lectoraten/smart-devices

Leukfeldt, R., van Eekelen, M., de Jong, E., & Vranken, H. (2012). Basic Cybercriminal Techniques & Techniques to cause Damage. In E. Leukfeldt, & W. Stol, *Cyber Safety: An Introduction* (pp. 167-168). Den Haag: Eleven International Publishing.

Lindenhout. (2016, november 6). *Onze organisatie*. Opgehaald van Lindenhout: https://www.lindenhout.nl/organisatie/onze-organisatie

Medisch spectrum Twente. (2017, juni 1). *Over MST*. Opgeroepen op juni 29, 2017, van MST: https://www.mst.nl/p/over-mst/

Nationaal Cyber Security Centrum. (2012). *Cybercrime, van herkenning tot aangifte.* Den Haag: Nationaal Cyber Security Centrum.

Nationaal Cyber Security Centrum. (2016). *Cybersecuritybeeld Nederland CSBN 2016.* Den Haag: Ministerie van Veiligheid en Justitie.

NEN. (2011, 1 Oktober). *Nen-shop*. Opgeroepen op Mei 24, 2017, van nen: https://www.nen.nl/NEN-Shop/Norm/NEN-75102011-nl.htm

Poel, P. v. (2017, Maart 6). *internet der dingen maakt opmars in de zorg.* Opgeroepen op Juni 2, 2017, van Skipr: https://www.skipr.nl/actueel/id29727-internet-der-dingen-maakt-opmars-in-zorg.html

Rahusen, P., & Reemer, R. (2010). *Whitepaper Patiënten- en informatielogistiek in de zorgsector.* 's Hertogenbosch: Ricoh.

Riskworld. (2015, juli 23). *de risico's van het internet of things*. Opgehaald van Riskworld: https://riskworld.nl/dossiers/integriteit/de-risico-s-van-het-internet-of-things

Santos, A. (2015, februari 2). *how to protect yourself against iot risks*. Opgehaald van securityintellegence: https://securityintelligence.com/how-to-protect-yourself-against-iot-risks/

Sincerus. (2017, februari 6). Opdrachtomschrijving. (J. Seegers, Interviewer)

Sincerus. (2017, januari 1). *organisatieprofiel*. Opgeroepen op februari 7, 2017, van Sincerus: https://www.sincerus.nl/organisatieprofiel/

SIS. (2015). *ISO 2022317.* Stockholm: Swedisch Standard Institute .

Smart-Homes. (2016). *Wat is domotica*. Opgeroepen op februari 13, 2017, van Smart-Homes: http://www.smart-homes.nl/Domotica/Wat-is-domotica.aspx

St. Jansdal. (2017, februari 2). *Karakteristieken*. Opgeroepen op juni 29, 2017, van St. Jansdal: https://www.stjansdal.nl/karakteristieken

Stoelinga, M. (2017 , Mei 11). Interview Marielle Stoelinga. (J. Seegers, Interviewer)

The Datacentergroup. (2016, Juni 13). *de gevaren van internet of things*. Opgeroepen op Juni 13, 2017, van thedatacentergroup: https://www.thedatacentergroup.nl/de-gevaren-van-internet-of-things/

Van Alphen, W., & Verhage, D. (2011). *Handboek risicobeheersing.* Zeist: Kerckebosch.

Van Beurden, M. (2014, 3 2). *computerwoordenboek*. Opgeroepen op Juni 7, 2017, van pc-tutorials: http://www.pc-tutorials.nl/computerwoordenboek.php

Van Dam, N., & Marcus, J. (2015). *Bron: Organisatie en Management; Nick van Dam en Jos Marcus.* Groningen: Noordhoff.

Van Rijsewijk, R. (2016). *Cyber Risico als Kans.* Amsterdam: Boom.

VMSzorg. (2017, december 12). *Platform voor patiëntenveiligheid*. Opgeroepen op maart 15, 2017, van vmszorg: http://www.vmszorg.nl/

Vranken, H. (2017, April 12). Interview Harald Vranken. (J. Seegers, Interviewer)

ZGT. (2017, maart 3). *over ZGT*. Opgeroepen op juni 29, 2017, van ZGT: https://www.zgt.nl/over-zgt/

Ziraonline. (2016, september 1). *Procesmodel*. Opgeroepen op maart 15, 2017, van Zirawiki: https://sites.google.com/site/zirawiki/procesmodel

Bijlages

Bijlage I Transcript Lodewijk Huinink MST

Sp1: Ik zou me allereerst even voorstellen. Ik ben Jeroen Seegers en 24 jaar. Ik studeer integrale veiligheidskunde op het Saxion te Deventer en ben nu aan het afstuderen bij Sincerus. Ik ben nu aan het afstuderen met als onderwerp: risico's bij het gebruik van smartapparatuur in het bedrijfsnetwerk, en dat in de zorgsector. Ik ga langs bij meerdere ziekenhuizen, zorgondernemingen en ik raadpleeg experts. Ik heb zelf een eigen definitie van smartapparatuur gedefinieerd omdat ik overal op internet een andere definitie tegen kwam. In samenwerking met Peter Westerveld ben ik tot de volgende definitie gekomen: *'Smartapparaten zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kunnen zijn op een intern netwerk en met elkaar kunnen communiceren.'* Het was de wens vanuit Sincerus dat er niet naar telefoons, computers en tablets wordt gekeken maar enkel naar de nieuwe generatie smartapparatuur.
Sp2: Heb je daar ook een voorbeeld van?
Sp1: Ja, slimme thermostaten en slimme verlichtingen.
Sp2: Ja, oké.
Sp1: Dus eigenlijk is het doel van dit onderzoek ook om te kijken, welke apparaten er allemaal voorkomen in dit ziekenhuis en welke categorieën. Ik heb een lijst samengesteld en dan kan ik daarbij langsgaan en dan kunt u misschien aangeven of het wel of niet aanwezig is binnen het ziekenhuis. Allereerst wil ik vragen: Bent u bekend met de term smartapparatuur?
Sp2: Het is inderdaad goed om een goede definitie te hebben alvorens je daarmee aan de gang gaat. Het is goed om te zeggen dat het geen pc's zijn, ofwel smartphones of tablets. Want deze worden er snel aan toegekend.
Sp1: Dus u bent er wel bekend mee?
Sp2: Ja, alleen ben ik wel sceptisch of wij deze apparatuur wel gebruiken.
Sp1: Oké, daar kunnen we straks misschien dan wel achter komen.
Sp2: Ja.
Sp1: Hoe bekend is uw organisatie met smartapparatuur?
Sp2: Beginnend. Mogelijkheden kunnen er zijn om ze te gebruiken maar naar mijn idee worden ze nog niet gebruikt. Vooral aan de business kant en aan de zorgkant zijn die vooruitgangen er al.
Sp1: Is er bij de bouw van het nieuwe ziekenhuis niet op ingespeeld?
Sp2: Bij de bouw is er met name van uitgegaan dat er een goede wifidekking is, en dat de infrastructuur daar op ingericht is. Ik schaar het eronder dat er op die manier aan is gedacht. Dus dat er een goede wifidekking is.
Sp1: Ik had ook gezien dat er in de toekomst echte 'smart hospitals' worden gebouwd. Dat is dit ziekenhuis dus niet?
Sp2: Het is geen primaire doelstelling.
Sp1: Dan zal ik nu de categorieën bij langs gaan en kunt u antwoorden of het er wel of niet is. Zijn er slimme thermostaten aanwezig?
Sp2: Niet dat ik weet.
Sp1: Slimme verlichting
Sp2: Niet dat ik weet.
Sp1: Slimme lampen. En dan bedoel ik bij de vorige systemen en bij deze categorie echt de lampen.
Sp2: Ik weet alleen dat wij bij de OK's…weet alleen niet of we die als slim mogen definiëren. Zit wel een systeem achter dat de kleur van de lichten kunnen worden aangepast, omdat als je vier uur lang aan het opereren bent je ander licht wil hebben dan daglicht. Maar deze staan niet in verbinding met het internet, dus dan valt deze niet onder de definitie van smartapparatuur.
Sp1: Slimme koelkasten?
Sp2: naar mijn weten niet
Sp1: wifikoelkast?
Sp2: Nee
Sp1: slimme wasmachines?

Sp2: nee, maar het zou kunnen. Dat zijn dan wasmachines die bij het ziekenhuis in de steriele omgeving kunnen zijn. Naar mijn weten niet. Als ze al verbonden zijn, dan zijn ze verbonden met het interne netwerk en niet naar buiten toe.
Sp1: Als het in verbinding staat met het intern netwerk dan schaar ik die ook onder smartapparatuur.
Sp2: Dan kan je die wel meenemen
Sp1: Weet u ook hoeveel?
Sp2: Nee, dat kan op één afdeling zijn maar die zitten niet onder ons beheer.
Sp1: Slimme drogers?
Sp2: Nooit van gehoord
Sp1: Slimme stofzuigers?
Sp2: Nee, nooit gezien
Sp1: Robot stofzuigers?
Sp2: Nee, nooit gezien
Sp1: Hebben jullie ook slimme deurbellen?
Sp2: Nee, niet in de zin dat je ergens op drukt om binnen te komen. Wij hebben hier een badgesysteem. Als je ergens naar binnen wil en als je er niet in komt dan is er niet een bel waardoor je alsnog binnen kan komen.
Sp1: Zijn er deuren die je kunt openen met je telefoon?
Sp2: Nee, alleen via die badge kan dat.
Sp1: Die staan in verbinding met het internet?
Sp2: Dat badgesysteem heeft een netwerkverbinding ja.
Sp1: Zijn er Smart-tv's aanwezig?
Sp2: Ja, we hebben wel tv's hier. Er zit een tv-signaal op patiënten tablets. Alle patiënten hebben een tablet tot hun beschikking waar ze eten op kunnen bestellen, tv kunnen kijken en radio op luisteren. Als ze een verpleegkundige nodig hebben kunnen ze die gebruiken als een soort bel.
Sp1: Zijn er daarnaast ook Smart-tv's aanwezig in vergaderruimtes of iets dergelijks waar je op kunt inloggen via een internetverbinding?
Sp2: Er zijn wel videoconferentiezalen met van die tv's, ik weet niet of je dat bedoelt?
Sp1: Het zijn gewoon televisies waar smartfuncties opzitten en internet.
Sp2: Die hebben we niet als dienst.
Sp1: zijn er ook slimme sloten in dit bedrijf?
Sp2: Als je die sloten bedoelt van het badgesysteem dan is dat een soort slot.
Sp1: Bij de ingangen?
Sp2: De hoofdingangen zijn 24 uur per dag open.
Sp1: Zijn er alarmsystemen en staan die in verbinding met het internet?
Sp2: Er zijn verschillende systemen. Je hebt een verpleegoproepsysteem. Een patiënt kan oproepen dat die hulp nodig heeft. En er is ook een brandalarm. Die staan allemaal in verbinding met een netwerk.
Sp1: Oké, valt het ook te scharen onder smartapparatuur? Waar wordt die verbinding voor gebruikt? Signalen naar de brandweer of iets dergelijks?
Sp2: Ik kan het me wel voorstellen maar weet het niet precies. Verpleeg oproepsysteem en medisch oproepsysteem is alleen intern.
Sp1: Je zou er niet binnen kunnen komen via een internetverbinding?
Sp2: Het staat wel geregistreerd en is een intern wifiverkeer. Via een Mos systeem krijgt de verpleegkundige op haar Mycom (Smartphone min). Geen apps op te downloaden. Er komt een melding op binnen dat er in een kamer een probleem is.
Sp1: Er zou een risico kunnen zijn dat de berichten worden beïnvloed. Wat zouden de gevolgen kunnen zijn?
Sp2: Het bericht kan worden aangepast naar verkeerd kamernummer. Of heel veel spookberichten die verzonden kan worden.
Sp1: Zijn er slimme tassen aanwezig?
Sp2: Nee.
Sp1: Zijn er smartwatches aanwezig die worden gedragen door medewerkers?
Sp2: Zou kunnen maar hebben geen functie. Die kunnen gewoon worden aangesloten op het gastnetwerk net als elk apparaat.

Sp1: Zijn er slimme stekkers aanwezig?
Sp2: Nee, niet gezien.
Sp1: Zijn er Slimme koffiezetapparaten aanwezig?
Sp2: Ze moeten eerst maar eens goede koffie zetten.
Sp1: Zijn er IoT-Sensoren aanwezig?
Sp2: Kan ik je niet zeggen, nee.
Sp1: Zijn er ook smart health apparaten?
Sp2: Ja dat is de 'Mycom'. Wat voorheen de pieper was is nu dat apparaat en dat zal ik je straks laten zien.
Sp1: Zijn er ook apparaten in operatiekamers die in verbinding staan met het internet? zoals monitoren van patiënten, elektriciteitsnetwerken?
Sp2: Die zijn gescheiden van elkaar.
Sp1: Heeft u zicht op alle smartapparatuur die gebruikt wordt door de medewerkers?
Sp2: Voor een deel, er is geen controle aan de poort. Dus alles wat buiten gebruikt wordt kan binnen ook gebruikt worden?
Sp1: Heeft u ook enig beleid omtrent smartapparatuur? Dat u tegen medewerker zegt let hier en hierop?
Sp2: Nee, je kunt ergens op inloggen of niet. Het beleid is waar je wel en niet op kunt inloggen.
Sp1: Als een nieuwe medewerker op het internet gaat zijn daar procedures voor?
Sp2: Je krijgt een inlogcode en dan krijg je rechten of je de mailbox wel of niet mag openen. Als je dus geen inlogcode hebt, dan kom je alleen op het gastnetwerk.
Sp1: Gastnetwerk staat niet in verbinding met vitale systemen?
Sp2: Nee, dat is een aparte lijn naar buiten.
Sp1: Daarnaast is er intern nog een aparte verbinding voor medewerkers?
Sp2: Ja, en voor apparatuur, en dat is onderverdeeld in freelance.
Sp1: Heeft u een overzicht van alle apparaten die in verbinding staan met het interne netwerk?
Sp2: Die gegevens zijn er wel.
Sp1: Dat kunt u niet vertellen? Of heeft u het niet helder?
Sp2: Per Macadres kan ik zien welke verbonden is.
Sp1: Moet u dat eerst opzoeken of heeft u een overzicht?
Sp2: Dat moet ik eerst opzoeken.
Sp1: Uit het gesprek komt al naar voren dat er niet veel smartapparatuur wordt gebruikt of dat u daar geen zicht op heeft. Toch wil ik vragen waar u op let bij de aanschaf van smartapparatuur? Of bent u daar niet verantwoordelijk voor?
Sp2: Ik ben daar niet verantwoordelijk voor.
Sp1: Weet u daar misschien iets van?
Sp2: De aanvraag gaat door naar de informatiemanager en de technische architect. Dan wordt er gekeken of het mag en of het kan.
Sp1: Wordt er gekeken naar de risico's van deze apparatuur?
Sp2: De impact wordt wel bepaald ja. Ook de Information Security officer wordt geraadpleegd en de TSO, Technical Security Officer.
Sp1: Wordt een apparaat ook getoetst aan bepaalde criteria?
Sp2: Deze wordt waarschijnlijk getoetst aan Nen-normen.
Sp1: Worden standaardwachtwoorden veranderd?
Sp2: Ik mag het hopen van wel. Ik kan het niet met zekerheid zeggen.
SP1: Bij andere DDoS-aanvallen is dit niet gebleken.
Sp2: Goede eerste check. Ik durf dit niet met zekerheid te zeggen.
Sp1: Ik had verwacht dat er meer smartapparatuur aanwezig zou zijn.
Sp2: Misschien heb ik niet het juiste beeld maar hier valt het nog wel mee.
Sp1: Heeft u zicht op de risico's van smartapparatuur?
Sp2: Ja maar dat is niet mijn domein. Ik ben incident en problemmanager. De ISO maakt zich er wel zorgen om en is daar wel kenbaar mee.
Sp1: Wat doet u als internetsystemen niet meer werken?
Sp2: Als escalatiemanager ben ik daar verantwoordelijk voor om zo snel mogelijk de dienst weer te laten uitvoeren waar het voor bedoeld is.
Sp1: Wat gebeurt er bijvoorbeeld als een internetsysteem uitvalt?

Sp2: Dan is bijvoorbeeld de patiënten informatie niet meer beschikbaar.
Sp1: Dat kan grote gevolgen hebben voor operaties en dergelijke?
Sp2: Als ergens anders een beeld is gemaakt die hier moet zijn bijvoorbeeld.
Sp1: Is dat dan ook het grootste risico, de patiënten informatie?
Sp2: Patiëntveiligheid is het grootste risico
Sp1: Zijn er naast de patiënten informatie nog andere componenten die de patiëntveiligheid beïnvloeden? Wordt er bijvoorbeeld ook digitaal geregeld wat de patiënt te eten krijgt?
Sp2: Ja, dat gaat via de tablet. Op die wijze bestellen de patiënten hun eten en drinken. Als dat niet beschikbaar is, is dat ze geen eten bestellen. Er is wel een noodprocedure, dan gaat iemand de kamers langs met de vraag wat ze willen eten en drinken. Maar dat is minder efficiënt.
Sp1: werkt de noodknop voor patiënten nog wel als er geen internet is?
Sp2: Dat werkt wel, als het niet via de wifi werkt dan krijgt de 'Mycom' een melding dat er geen wifiverbinding is. Dan moeten de verplegers op kamerlamp lopen. Er gaat een lamp branden bij de kamers en de 'Mycom' krijgt normaalgesproken een signaal.
Sp2: Er moet fysiek gekeken worden naar waar het lampje brand. Dat noemen wij op kamerlamp lopen.
Sp1: Is het niet achterhaald?
Sp2: Er zijn verschillende systemen. Je hebt het verpleegoproepsysteem. Als het goed werkt krijg je op je 'Mycom' te zien waar je heen moet zijn. Dat is per afdeling lopen op lamp als deze niet werkt. En je hebt het mos systeem Noodprocedure zodat je op de centraalpost moet gaan zitten.
Sp1: Hoe is de bewust zijn de medewerkers van cyberrisico's?
Sp2: Op een schaal van niet tot hoog, is het bewustzijn laag tot midden.
Sp1: Wat is daar de oorzaak van?
Sp2: Men weet dat het kan gebeuren maar niet zo zeer dat het in een ziekenhuis kan gebeuren en welke gevolgen het kan hebben.
Sp1: Besteden jullie daar geen aandacht aan richting de medewerkers?
Sp2: Te weinig
Sp1: Er zijn zich dus wel degelijk een aantal mensen bewust dat het ziekenhuis slachtoffer kan worden van cybercriminaliteit?
Sp2: Ja, een veiligheidsaspect is de ransomware bijvoorbeeld. Daar wordt weleens in de twee maanden melding van gemaakt met de boodschap: Let op, wat niet voor jou is en wat een aparte afzender heeft, niet openen en gooi weg. Maak er melding van maar stuur niet de bijlage mee. Maar niet in de zin of je 'Mycom' gehackt kan worden.
Sp1: Waarom denkt u dat uw organisatie slachtoffer zou kunnen worden van cybercriminaliteit?
Sp2: Omdat ze denken geld er mee te kunnen verdienen, niet zo zeer om de informatie die beschikbaar is. Dat is de grootste reden. Dat verdienen ze bijvoorbeeld door ransomware te versturen.
Sp1: Kan het ook zo zijn dat Kwaadwillenden de patiënten iets aan willen doen?
Sp2: Het zou kunnen, maar dat zijn allemaal risico's die zouden kunnen. Belangrijke informatie die nodig is voor zorgverzekeraars zou ook gehackt kunnen worden. Het zou allemaal kunnen.
Sp1: Hebben er incidenten plaatsgevonden binnen dit ziekenhuis?
Sp2: Er zijn wel wat incidenten geweest qua informatiebeveiliging?
Sp1: Waren dat er veel of weinig?
Sp2: Weinig. We hebben weleens met een ransomware te maken gehad.
Sp1: Is er ook een business continuity plan aanwezig binnen het bedrijf voor de cyberveiligheid?
Sp2: Er is een plan, het uitvallen van de ICT kan je er onder scharen
Sp1: Hoe gaat het in zijn werk?
Sp2: Op strategische punten zorgen we ervoor, dat er elektronische beschikbaarheid is van patiëntendossiers van een x-aantal uren vanaf dat moment.
Sp1: Dus als er een systeem uitvalt zorgt u ervoor dat er back-ups zijn?
Sp2: Ja, die draaien op een ander netwerk en kunnen ook nog stand alone draaien.
Sp1: Heeft u ook gegevens, voor de zekerheid, hard copy?
Sp2: De gegevens zitten enkel op stand alone computers.
Sp1: Wat betekend stand alone?
Sp2: Computers die separaat kunnen draaien van een netwerk.
Sp1: Als er vitale systemen uitvallen? Als er bijvoorbeeld elektriciteit uitvalt.

Sp2: We hebben normale noodvoorzieningen. Zoals noodstroom.
Sp1: Bent u bang dat er in de toekomst nog meer problemen zullen ontstaan op dit gebied?
Sp2: Het probleem wordt niet kleiner. Op securitygebied wordt het alleen maar groter. Je moet er voor waken en je moet je ertegen beschermen.
Sp1: Hoe wilt u als ziekenhuis met die trend mee gaan zodat alles wel veilig blijft?
Sp2: Er zal meer aandacht komen en er zal een groter budget voor zijn.
Sp1: Zal er in de toekomst een groter draagvlak voor zijn?
Sp2: Ja dat denk ik wel.
Sp1: Wordt er ook gekeken naar het falen van de mens bij cyberrisico's?
Sp2: Ja, beveiliging begint bij jezelf. Je kunt alles goed bewaken. Het begint met wachtwoorden op een kladje schrijven. Er wordt aangegeven omdat niet te doen, omdat je eigen veiligheid er ook mee te maken heeft. Er het geschreven beleid wordt gehandhaafd.
Sp1: Worden er ook trainingen over gegeven?
Sp2: Niet standaard.
Sp1: Heeft elke medewerker te maken met het internet? Iedereen heeft dus zo'n 'Mycom'?
Sp2: Nee, de verpleegkundige hebben een 'Mycom'. Die zijn niet persoonlijk maar die zijn verdeeld per afdeling.
Sp1: Kan de 'Mycom' onder smartapparatuur geschaard worden?
Sp2: Ja, als je erover twijfelt zou ik zeggen, ja.
Sp1: Een kleine samenvatting van wat u gezegd heeft: U zegt dat er eigenlijk weinig smartapparatuur binnen de organisatie zijn. De bekendheid is nog niet erg groot en u bent zelf nog niet echt bekend met deze apparaten. Medewerkers zijn zich wel een beetje bewust maar niet bewust genoeg van het feit dat ze risico lopen op hacken. Patiëntveiligheid is het belangrijkste doel en de hackers hebben als doel om geld te verdienen via ransomware of DDoS aanvallen. De grootste risico's zijn de 'Mycom's.
Sp2: Dat klopt.
Sp1: Voor de rest ziet u niet echt grote risico's?
Sp2: Nee, want als tablets, pc's en smartphones niet worden meegenomen, niet.
Sp1: Denkt u dat de standaard beveiliging van het ziekenhuis goed is?
Sp2: Ik denk dat je die per half jaar moet checken of deze nog steeds up to date is met wat er in de buitenwereld beschikbaar is.
Sp1: Via het gastnetwerk kan je nergens bij komen?
Sp2: Niet intern, je gaat alleen naar het internet.
Sp1: Zijn er ook medewerkers die met vertrouwelijke informatie moeten werken? Zijn daar procedures voor?
Sp2: Ja die zijn er.
Sp1: Is het een risico dat intern medewerkers, data kunnen lekken en is de organisatie zich daar bewust van? Hoe wordt daarop ingespeeld?
Sp2: Dat kan. Je moet zorgen dat je een zorgrelatie hebt met de patiënt. Er bestaat de mogelijkheid dat je die informatie kan lekken. Het wordt gelogd wie waar en wanneer bij patiëntgegevens kijkt.
Sp1: Is dat een kwestie van vertrouwen of zijn er echt zware regels voor? Zijn er harde maatregelen getroffen?
Sp2: Ik ken de procedures niet zo duidelijk dat ik daar een antwoord op kan geven.
Sp1: Heeft u nog aanvullende informatie?
Sp2: Een ziekenhuis is openbaar dus alles van buiten kan ook zo naar binnen.
Sp1: Hoe is het gesteld met de fysieke beveiliging?
Sp2: Daar is dus het badge systeem voor wat gehandhaafd moet worden. Er is ook een overzicht wie welke badge heeft. De fysieke beveiliging is wel in orde, maar als ik mijn pasje kwijtraak, dan kan iemand anders met mijn pasje overal binnen komen. Er is niet zoiets als een tweede code. Als dit gebeurd dan wordt het pasje geblokkeerd. Het moet wel gedaan worden. Er wordt niet gemonitord dat ik een pasje kwijt ben.
Sp2 Je kan op elke openbare ruimte komen zonder pasje. Alleen niet op de OK. Overdag zijn alle deuren open voor de ICT-afdeling. 's Avonds gaan de deuren dicht. We hebben gezegd; iedereen mag hierbinnen komen. Er is niks te halen behalve persoonlijke spullen zoals een laptop. Via de computers kom je niet

binnen op het interne netwerk omdat je moet inloggen met een pasje en je moet om de vier uur je wachtwoord invoeren.
Sp1: De beveiliging is dus wel heel hoog?
Sp2: Je moet een goede afweging maken tussen veiligheid en dat het werkbaar blijft. Er wordt wel aandacht aan besteed maar het mag altijd meer zijn.
Bij de rondgang door het ziekenhuis zijn nog smartapparatuur ontdekt; Er zijn vier vergaderruimtes waar in totaal ongeveer tien smart-tv's hangen en er hangt een digitaal agenda systeemkastje bij het atrium. Deze staan in verbinding met het internet.

Bijlage II Transcript Gea Wijn Deventer Ziekenhuis

SP1: Ik ben Jeroen Seegers en ik ben 24 jaar. Ik ben aan het afstuderen voor de opleiding integrale veiligheidskunde bij Sincerus consultancy in Zwolle. Dat is een informatiebeveiligingsbedrijf waar onder andere advies wordt gegeven, pentesten worden uitgevoerd en mystery guest operaties worden gedaan. Mijn onderzoek gaat over de risico's bij het gebruik van smartapparatuur in een bedrijfsnetwerk in de zorgsector. Dan ga ik bij een aantal ziekenhuizen en een aantal zorgondernemingen kijken wat de rol van smartapparatuur is. Ik kijk ook wat de risico's daarvoor zijn en in het bijzonder de kritische processen. Het belangrijkste aspect is de patiëntveiligheid die daarbij komt kijken. Ik zou u dus graag willen interviewen over de kritische processen van een ziekenhuis omdat Wim Smeitink aangaf dat Leon Bosch hier ooit een onderzoek heeft gedaan omtrent kritische processen en dat u zijn begeleider was. Hij gaf aan dat ik een interview moest proberen te regelen om veel te weten te komen over kritische processen. Dus, zodoende. Kunt u wat over uzelf vertellen?
SP2: Ik ben Gea Wijn. Ik ben milieu en BHV-coördinator en ik heb eigenlijk drie aandachtsgebieden binnen het ziekenhuis. Bij milieu moet ik ervoor zorgen, dat het ziekenhuis zich aan de milieuvergunning houdt en daarbij komt ook een stukje duurzaamheid om de hoek kijken. We zijn heel voorzicht met duurzaamheid bezig. Daar ben ik bedrijfsbreed coördinator voor. Dan het stukje BHV; Ik ben hoofd BHV van zeventig BHV-ers. Dit is ook bedrijfsbreed. Ik organiseer opleidingen, trainingen, oefeningen en ik zorg dat het functioneren van de BHV georganiseerd zijn. Ik zorg voor de middelen, spullen en dergelijke. Als derde aandachtsgebied heb ik het ziekenhuisrampenopvangplan c.q. crisisplan. Ik ben daarvoor ook ziekenhuisbreed coördinator. We hebben een ziekenhuisrampenopvangplan (afgekort ZIROP) en we zijn nu een doorgroeitraject aan het doormaken naar een integraal crisisplan.
SP1: Doet u dat alleen of doet u dat met meerdere?
SP2: Nee. We hebben een crisisplancommissie dus we doen het met meerderen.
SP1: Heeft u een eigen afdeling binnen het ziekenhuis?
SP2: Nee, ik val onder het facilitair bedrijf in mijn functie. Voor het stukje crisisplan/ZIROP val ik informeel onder de zorgmanager die de acute intensieve afdelingen onder zijn aandachtsgebied heeft. Die is ook tevens de voorzitter van die crisisplancommissie c.q. ZIROP-commissie.
SP1: Hoe zien de kritische processen van een ziekenhuis eruit?
SP2: Kritische processen zijn processen waarbij de zorgcontinuïteit c.q. patiëntveiligheid niet of niet voldoende worden geborgd. We hebben kritische processen en kritische voorzieningen onder één noemer gegooid. We hebben per verschillende bedrijfsonderdelen een risicoanalyse laten doen. Dat heeft Leon Bosch gedaan. Leon heeft de risicoanalysemethode ontwikkeld en heeft deze vervolgens toegepast op de ICT en technische dienst afdeling. Voor hun processen, wat zijn voor hun kritische punten en waar lopen ze risico? Waarop je de zorgcontinuïteit c.q. patiëntveiligheid niet voldoende kan borgen. Daarna is er een volgende stagiair gekomen en die heeft dezelfde risicoanalyse toegepast voor het facilitair bedrijf. De volgende stap is de afdeling ic en CCU(hartbewaking). Als laatste bij de andere overige afdelingen. Uit deze risicoanalyses komen allemaal kritische processen en dat is per bedrijfsonderdeel verschillend.
SP1: Dus je kunt niet zeggen de kritische processen van een ziekenhuis ziet er zo uit? Er zijn wel algemene processen natuurlijk. Het primaire proces is zorg verlenen?
SP2: Ja maar je hebt bij zorg verlenen bijvoorbeeld bepaalde voorzieningen nodig. Je bent afhankelijk van netvoorzieningen. Waarbij stroom en drinkwater echt invloed hebben op de patiëntveiligheid of zorgcontinuïteit. Gas is minder want dat gebruiken we hier voor verwarming en daar kunnen patiënten wel even zonder. Medische gassen zoals zuurstof die heb je op bijna alle afdelingen wel nodig. Als dat uitvalt, dan moet een afdeling zelf acties ondernemen om ervoor te zorgen dat de patiënten geen schade ondervinden. De zuurstofvoorziening is wel een kritisch proces of een kritische voorziening. Je kunt het op meerdere manieren benoemen en dan hebben we als vervolg op de risicoanalyse voor de risicovolle voorzieningen of processen continuïteitsplannen gemaakt met actiekaarten. De IC heeft nu de kaarten voor als de stroom uitvalt en dan gaan we er ook van uit dat de back-up voorzieningen niet goed functioneren dus dat een ic-verpleegkundige moet handelen in een situatie als die helemaal geen stroomvoorziening meer heeft. Wat valt er dan uit? Welke cruciale apparatuur of middelen heb je niet meer tot je beschikking? Dat zal je in gang moeten zetten. Op die manier hebben we dat vormgegeven. De technische dienst heeft hier heel veel noodvoorzieningen voor al dat soort belangrijke processen en

zolang alles het doet hoeft de verpleegkundige daar niks van te merken. De verpleegkundige hoeft dan geen actie te ondernemen. Als dat uitvalt moet de verpleegkundige weten welke mogelijkheden die heeft.
SP1: Is dat per afdeling zo verschillend of zijn er dingen die wel overeenkomen?
SP2: Dat ligt er dus aan als je afdeling hebt waar geen zuurstofbehoeftige patiënten hebt dan is de zuurstof op dat moment dus niet zo kritisch. Stroom is dan ook niet heel erg kritisch. Je wil natuurlijk wel je ICT-voorzieningen in de lucht hebben. Op het moment dat je helemaal geen stroom hebt en ook het netwerk uitvalt, zie je daar het grootste probleem.
SP1: Zo'n zuurstofvoorziening staat die in relatie met het elektriciteitsnetwerk?
SP2: Nee, dat niet. Daar is geen elektriciteit bij nodig.
SP1: Welke kritische processen lopen het meeste risico?
SP2: De stroomvoorziening, maar daar hebben we ook een noodstroomaggregaat voor. Op het moment dat die uitvallen dan heb je een tweede probleem. Op het moment dat de externe stroomvoorziening uitvalt, heb je in principe je noodstroom. Toch hebben we dus daar in die risicoanalyse gekeken naar; als de noodvoorziening het niet doet, wat betekend dat voor je patiëntveiligheid en zorgcontinuïteit.
SP1: Het is echt op de ICT toegepast?
SP2: Klopt, maar ook bij de facilitaire dienst. Die zorgt bijvoorbeeld voor de hele voeding in het ziekenhuis. Daar heb je koelkasten voor nodig en daar heb je elektrische apparatuur voor nodig omdat te regenereren. In die zin heeft het facilitair bedrijf ook last van uitval van dat soort voorzieningen. Voor parkeren is het zo dat slagbomen niet meer opengaan. Voor beveiliging heb je de kans dat de camera's uitvallen. Zo heb je in elk bedrijfsonderdeel wel weer wat andere kritische systemen.
SP1: De een is denk ik belangrijker dan de andere, omdat er bij de een slachtoffers kunnen vallen en bij de ander niet? De ICT is toch eigenlijk een ondersteunend proces van het primaire proces? Dus zijn de ondersteunende processen in kaart gebracht die de primaire processen ondersteunen?
SP2: Als eerste is dat inderdaad gebeurd. Vervolgens is er daarna nog op de afdelingen zelf nog een analyse gedaan.
SP1: Welke processen vinden jullie zelf het belangrijkst binnen het ziekenhuis?
SP2: ICT is een belangrijke voorziening. Dat is het proces waarmee je alle patiëntgegevens registreert. Alle onderzoeksresultaten en dergelijke. Als dat uitvalt dan heb je een probleem. We zijn geheel digitaal en er zijn eigenlijk geen papieren dossiers. Er zijn wel back-up stations in huis maar die zitten zo maximaal mogelijk uit elkaar. Als dat uitvalt dan heb je daadwerkelijk wel een probleem voor de zorgcontinuïteit, want daar staat ook bijvoorbeeld medicatie in genoteerd en diëten staan erin genoteerd.
SP2: Ja. Daar aangekoppeld; het apothekerssysteem en het voedingssysteem.
SP1: Oké, dat gaat allemaal digitaal?
SP2: Ja
SP1: In welke mate is dat beveiligd? Hoe spelen jullie in op de mogelijke risico's dat het gevaar kan lopen?
SP2: Daar kan ik jou technisch inhoudelijke geen antwoord op geven. Daar hebben we de collega's van ICT voor nodig.
SP1: Oké. Wordt er wel aandacht aan besteed?
SP2: Jazeker.
SP1: Welke factoren hebben invloed op de patiëntveiligheid?
SP2: Dat zijn dus voorzieningen maar dat is afhankelijk van wat de patiënt nodig heeft. Als de patiënt hier ligt dankzij een knieoperatie zal deze niet zuurstofafhankelijk zijn. Als deze patiënt geen diëten heeft en deze krijgt therapie, eten en drinken, dan kan er niet zoveel fout gaan. Als je een patiënt hebt die kritisch is, zoals op ic, die wel zuurstofbehoeftig is en aan allerlei registratieapparatuur hangt voor zijn vitale functies, dan ben je echt super afhankelijk van stroomvoorziening of batterijen en accu's. Daarnaast ben je ook afhankelijk van je patiënten informatiesysteem.
SP1: Helpen jullie als de stroom bijvoorbeeld uitvalt als eerst de meest kritische patiënten? Hoe prioriteren jullie dat?
SP2: Ja. Zulk soort apparaten zijn voorzien van een accu. Daardoor heb je 2 uur uitstel voordat de hele boel uitvalt. Wat betreft het netwerk durf ik niet te zeggen of daar ook een batterijvoorziening achter zit.
SP2: Op welke manier wordt op dit moment de patiëntveiligheid gewaarborgd?
SP1: Door dat we voor verschillende belangrijke voorzieningen back-up voorzieningen hebben en daarop weer noodprocedures hebben gemaakt in de techniekssfeer. ICT en TD heeft allemaal noodprocedures en

noodplannen gemaakt en daar wordt preventief onderhoudt gepleegd om te zorgen dat alle belangrijke voorzieningen in de lucht blijven.
SP1: Worden de in kaart gebrachte processen wel weer herzien of is het een keer gemaakt en klaar?
SP2: Nee. We moeten dat eens in de zoveel tijd weer checken of dat nog klopt, maar zover zijn we nog niet.
SP1: Moet dan de hele organisatie eerst in kaart worden gebracht voor dat je een check kan doen?
SP2: Of de hele organisatie in kaart wordt gebracht betwijfel ik omdat nu de voornaamste afdelingen zijn gedaan. Het is mogelijk dat we nog een vervolg doen op de operatieafdeling maar in feite als je de ic, de algemene afdeling en de ondersteunende afdelingen hebt gedaan dan verwachten we niet dat we zoveel hebben gemist.
SP1: Hebben jullie alle processen in eigen beheer of zijn er ook dingen uitbesteed?
SP2: We hebben de organisatie in eigen beheer maar er is wel een installateur bijvoorbeeld die ingehuurd wordt voor allerlei operationele klussen. De organisatie is eigen beheer. We besteden geen logistiek uit en we hebben geen medewerkers van de technische dienst ingehuurd.
SP1: Hoe groot is dit ziekenhuis eigenlijk?
SP2: We hebben 380 bedden. 1200 FTE aan medewerkers.
SP1: Is dit een ziekenhuis waar je alle zorg kan krijgen?
SP2: Niet helemaal alles, maar wel grotendeels. We hebben ook samenwerkingen met nabijgelegen ziekenhuizen. Vakgroepen onderling delen expertise uit zodat het specialisme wel het minimumniveau haalt qua behandelingen. Als je niet een aantal behandelingen haalt kan je niet je specialisme van het ziekenhuis behouden. Middels samenwerkingen met naastgelegen ziekenhuizen kan je dat borgen.
SP1: Hoe zit het met de organisatie van het ziekenhuis? Is dat één grote organisatie of zijn het meer eilandjes op zichzelf?
SP2: Wij hebben wel verschillende bedrijfsonderdelen, met de bedoeling dat je goed met elkaar samenwerkt en dus geen eilandje bent. We hebben het facilitair bedrijf, we hebben ICT en TD en we hebben de zorg. Daar valt alles onder die met patiënten te maken hebben. Daarnaast hebben we nog een afdeling die heet paramedische dienst. Dat is fysiotherapie, diëtetiek en ergotherapie. We hebben ook nog financiën en inkoop.
SP1: Per onderdeel heeft u het proces in kaart gebracht maar zijn deze processen ook aan elkaar gekoppeld en waar blijkt dat uit?
SP2: Deels wel. Afdeling ICT die zorgt dat systemen beschikbaar en bereikbaar zijn. Het facilitair bedrijf heeft het weer nodig voor de voeding wat weer gerelateerd is aan de zorg.
SP1: Is er een business continuity plan aanwezig en hoe ziet deze eruit?
SP2: Daar zijn we dus mee begonnen maar dat is nog niet bedrijfsbreed. Er zijn al wel een boel beheersplannen om de voorzieningen in de lucht te houden. Dat heeft eigenlijk ook alles met business continuity te maken. Dat zijn onderdelen, het zijn deelplannen die eronder vallen. We zijn bezig om te groeien naar een integraal crisisplan en daarin wordt ook de continuïteit benoemd en die is dus recentelijk gestart. Van daaruit willen we op basis van de risicoanalyses die we nu hebben gedaan, de bedrijfscontinuïteit verder uitrollen.
SP1: Hoe zorg je er als organisatie dan voor dat de kritische processen niet uitvallen voor dat je naar het continuïteitsplan gaat?
SP2: Door dus beheersplannen te schrijven daarvoor en ervoor te zorgen dat je de nodige back-up voorzieningen hebt.
SP1: Back-ups zijn dus het belangrijkste om ervoor te zorgen dat processen niet worden onderbroken.
SP2: Wat daar ook mee samenhangt, is dat er aan applicaties een servicelevel niveau moet hangen wat ook voldoende urgentie heeft. ICT heeft voor verschillende applicaties servicelevels opgesteld. De meest belangrijke applicaties krijgt servicelevel 5 en de minst belangrijke applicaties servicelevel 1. Als er een storing is, dan is het afhankelijk van de servicelevel hoe snel het moet worden hersteld.
SP1: Wat bedoelt u met applicaties?
SP2: Dat is bijvoorbeeld het dieetsysteem waar alle dieetvoedingen aan gekoppeld zijn of het patiëntgegevenssysteem of apothekerssysteem.
SP1: U zei net dat er geen papieren back-ups zijn? De back-ups zijn dus ook digitaal?
SP2: Er worden voor een aantal zaken wel lijsten uitgeprint voor het geval iets uitvalt en je van je intranet verstoken bent. Over het algemeen is alles digitaal en werken we ook digitaal.

SP1: Als de patiëntendossiers niet beschikbaar zijn dan kunt u nog wel bij die gegevens?
SP2: Nee, dat is lastig. We hebben wel een externe locatie waar eventueel back-ups kunnen worden gegenereerd. Ik weet dat ze op dit moment bij ICT bezig zijn om een voorziening te maken, waarbij je vanaf een externe locatie bij het patiënten systeem kunt. Als er in het ziekenhuis een calamiteit is dat je vanaf extern toch nog kan inloggen. Het kan zijn dat je alle patiënten moet ontruimen en naar een ander ziekenhuis moeten dan zit je met zo'n dossier. Je hebt geen map meer waar alles in staat. Nu zijn we aan het regelen dat je vanaf een ander ziekenhuis kan inloggen op ons patiënte systeem om daar ook de benodigde gegevens bij de hand te hebben.
SP1: Dit betreft dan alleen een fysieke calamiteit. Als er bijvoorbeeld een hacker is geweest die informatie versleuteld dan kan het externe ziekenhuis er toch ook niet bij? Dat is dan wel een risico denk ik?
SP2: Daar kan ik je geen antwoord op geven. Dan moet je echt bij de ICT zijn.
SP1: Hoe bewust zijn de medewerkers zich van kritische processen en patiëntveiligheid?
SP2: Daar worden ze wel in geschoold.
SP1: Op wat voor manier?
SP2: Op verschillende vlakken. De afdeling die nu die continuïteitsplannen hebben (die actiekaarten) daarvan worden medewerkers in geschoold wat dat inhoud, wat dat voor hun betekend en wat ze daar voor rol in hebben. Er is een scholingsprogramma betrekking tot brandveiligheid en risico's. Dat medewerkers zich bewust zijn van hun handelwijze en hun rol met betrekking tot het terugdringen van een calamiteit. Zo dat je het ontstaan van een calamiteit zoveel mogelijk inperkt. Wat betreft de informatievoorziening wordt er gehamerd op dat wanneer je weg loopt van je werkplek je, je beeldscherm en computer afsluit. Zo niet dan krijg je een rode kaart. Dat houdt niet in dat je een boete moet betalen maar het is een bewustwordingsproces. Als je de computer niet afsluit dan kan iemand anders die daar zo rondloopt, inzage kunnen krijgen in patiëntgegevens. Op die manier is er echt een aanspreek cultuur naar elkaar toe en pas op dat je goed om gaat met je gegevens.
SP1: Werkt dat systeem goed en is de situatie verbeterd?
SP2: Jawel en het is ook verbeterd.
SP1: Hoe gaan jullie om met menselijk falen? Een mens maakt namelijk fouten.
SP2: We hebben een veiligheid informatie managementsysteem. Als iemand een fout maakt moet die dat melden via een VIM Melding. Dat is een laagdrempelig, ziekenhuisbreed, meldsysteem waar grote fouten worden gemeld die dan worden geëvalueerd. Daar worden dan verbeteracties uit benoemd die dan weer in jaarplannen terecht komen. Op die manier probeer je de PDCA Cyclus rond te krijgen, zodat je leert van fouten.
SP1: Worden er dan ook trainingen gegeven? Ze worden ook geschoold, maar wordt er ook aandacht aangegeven aan de menselijke kant? De human factors?
SP2: Ja.
SP1: Houden jullie je ook bezig met de belangrijke VMS-thema's?
SP2: De VMS-thema's zijn leidend voor ons kwaliteitsmanagementsysteem. Ik ben ook interne auditor voor kwaliteitssysteem. We hebben een kwaliteit coördinator die bedrijfsbreed het kwaliteitssysteem beheerd. We zijn NIAS gecertificeerd. Die VMS-thema's/ Lopen door rode draad door het hele kwaliteitssysteem. Bij interne audits worden specifiek die VMS-thema's ook weer meegenomen.
SP1: Kunt u ook wat vertellen over hoe je incidenten voorkomt bij high risk medicatie of het verwisselen van patiënten?
SP2: Er zijn dus protocollen op geformuleerd, maar daar kan ik inhoudelijk niets over zeggen. Ik weet dat ze er zijn en dat mensen zich daaraan moeten houden en als dit mis gaat wordt het weer via de VIM gemeld. Zo gaat die cyclus weer rond.
SP1: Als er bijvoorbeeld cybercriminelen via smartapparatuur het bedrijfsnetwerk in kunnen, dan kunnen ze dus bij patiëntgegevens, medicijngebruik en voedselaanbod komen. Dit kan resulteren in dat de patiënt verkeerde medicijnen of voedsel toegediend krijgt of dat de informatie versleuteld wordt. Dat kan natuurlijk levens kosten. Hoe denkt u dat er mee omgegaan moet worden om deze situaties te voorkomen?
SP2: ICT moet daar bepaalde veiligheidssystemen voor hebben ontwikkeld. Ik kan daar verder niets over zeggen.
SP1: Ik wil u nog een aantal vragen van de risicoanalyse voorleggen. Welke situaties proberen we te voorkomen?

SP2: We proberen te voorkomen dat het systeem gehackt wordt.
SP1: Welke partijen zijn verantwoordelijke?
SP2: ICT en TD zijn heel belangrijk daarin. Raad van bestuur is eindverantwoordelijk.
SP1: Welke externe ontwikkeling kunnen mogelijk tot kwetsbaarheden lijden?
SP2: Je gaat natuurlijk steeds verder met je patiëntbenadering door middel van internet. Je kunt je eigen dossier thuis inzien, afspraken worden digitaal gemaakt, huisartsen kunnen afspraken inplannen. Je gaat steeds meer digitaal infiltreren in de bevolking. Dat lijkt me een uitdaging omdat goed te beveiligen.
SP1: Welke typen dreigingen kunnen zich nu en in de toekomst voordoen?
SP2: Een cyberaanval, maar daar heb ik verder geen zicht op.
SP1: Heeft u daar helemaal geen contact over met ICT?
SP2: Nee tot nu toe nog niet. We hebben de werkgroep continuïteit en daar ga ik nog ingroeien.
SP1: In de toekomst zal het waarschijnlijk het belangrijkste risico worden. Wat zou de impact kunnen zijn van die risico's?
SP2: Als je patiënten informatiesysteem plat ligt zal dat kunnen betekenen dat patiënten niet meer de juiste zorg krijgen.
SP1: Hoe breng je dreigingen in kaart?
SP2: Onder andere Door het maken van risicoanalyses. Hoe ICT dat doet, kan ik je niet zeggen.
SP1: Welke maatregelen worden er toegepast voor het beveiligen van de processen?
Sp2: In kaart brengen, back-ups, beheersplannen en protocollen ontwikkelen.
SP1: Wat zal volgens u een maatregel kunnen zijn als smartapparatuur risico's met zich meebrengen wanneer het gebruikt wordt in een intern netwerk.
SP2: Dat zal afgeschermd moeten worden maar ik kan er verder geen antwoord op geven.
SP1: Hoe belangrijk zijn secundaire processen voor de primaire processen?

SP2: Je kunt nog wel wat maar ze werken niet voldoende. De zorg kan niet meer voldoende gebord worden. De zorgcontinuïteit en patiëntveiligheid kunnen niet geborgd worden.
SP1: Is het proces in elk ziekenhuis hetzelfde? Verschilt het per grootte?
SP2: Iedereen komt overal binnen met een zorgvraag dus is het overal hetzelfde.
SP1: Is dat hetzelfde bij particuliere zorgondernemingen?
SP2: Ja het proces is hetzelfde. Er is een zorgvraag en de vervolgstappen zijn bijna hetzelfde.
SP1: Is het een verschil dat er in het ziekenhuispatiënten zijn die een levensbedreigende situatie hebben en in een zorgonderneming niet?
SP2: Dat zou het enige verschil dan zijn.
SP1: Dit was alles wat ik wilde weten. Ik heb nog een aantal vragen maar die kan ik beter aan mensen van ICT stellen. Bedankt voor de informatie en uw tijd.
SP2: Graag gedaan.

Bijlage III Transcript interview Harald Vranken

SP1: Dan ga ik gelijk beginnen. Kunt u wat over uzelf vertellen, over uw achtergrond en uw vakgebied?
SP2: Ja. Ik ben werkzaam als universitair hoofddocent aan de Open Universiteit en daarnaast ben ik ook één dag in de week aangesteld aan de Radboud Universiteit. Ik hou mij bezig met security van computers en informatiesystemen. Afgelopen jaar heb ik met name gekeken naar labs waar security experimenten kunnen worden gedaan door studenten of om experimenten uit te voeren. Daarnaast heb ik gekeken naar security van online bankieren. Momenteel werk ik aan botnetdetectie waar de vraag is of je aan de hand van internetverkeer dat je kan observeren en organiseren, of je daar met machinetechnieken botnets in kan detecteren. Ik werk nu zo'n tien jaar in dit vakgebied aan de open universiteit. Daarvoor heb ik gewerkt bij Phillips research. In de hoek van het ontwerpen van chips en daarvoor heb ik gestudeerd aan de TU Eindhoven.
SP1: U werkt ook bij Cyber Science Center toch?
SP2: Ja, Cyber Science Center is geen instituut met werknemers. Het is een samenwerking van onderzoekers van diverse instituten. Het is niet iets waar je formeel wordt aangesteld voor een bepaalde tijd. Ik ben inderdaad wel verbonden aan het CSC.
SP1: Klinkt allemaal interessant. Ik heb een eigen definitie gehanteerd voor de term smartapparatuur omdat overal in literatuur andere omschrijvingen worden gebruikt. Ik zou deze even voorlezen. 'Smartapparatuur zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kan uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kan zijn op een intern netwerk en met elkaar kunnen communiceren.' Deze heb ik zo opgesteld omdat mijn opdrachtgever het belangrijk vond dat ik niet de telefoons, laptops en tablets zou meenemen in het onderzoek. Het gaat echt om de nieuwe generatie slimme apparatuur zoals slimme meters, slimme stofzuigers die thuis ook te vinden zijn. Hoe bekend bent u met de term 'Smartapparatuur'?
SP2: Smartapparatuur ben ik zelf niet mee bekend. Ik ben wel bekend met het woord smart dat in deze context wordt gebruikt. Daar ken ik het wel van.
SP1: Hoe zou u het zelf omschrijven? Het wordt vergeleken met Internet of Things maar er zitten toch kleine verschillen in. Hoe ziet u dat?
SP2: Nou ik heb er niet diep over nagedacht maar als ik het zo voor de vuistweg zou moeten omschrijven denk ik dat smart aangeeft dat een apparaat een zekere intelligentie bezit. Die intelligentie wordt bereikt door een computersysteem die er in zit, die kan processen met een geheugen en met de buitenwereld kan communiceren. Zo zou ik het denk ik willen omschrijven. Volgens mij ligt dat heel dicht tegen de definitie aan die jij net noemde.
SP1: Oké, hoe zorg je ervoor dat informatiebeveiliging goed is afgesteld op kritische processen van een organisatie?
SP2: Relateer je deze vraag aan smartapparatuur of breder?
SP1: Breder. Algemene informatiebeveiliging van een bedrijf. Hoe zorg je ervoor dat die goed is afgesteld zodat je kritische processen geen gevaar lopen?
SP2: Dat is een vraag die niet zo één, twee, drie te beantwoorden valt denk ik. Er spelen een aantal zaken een rol. Ik denk zoals altijd dat de security de basis is voor een goede riskmanagement. Je moet weten wat zijn mijn assets, wat is kritiek in mijn waardevolle gegevens, waardevolle systemen en wat is de waarde daarvan. Aan de hand daarvan moet je beleid gaan bepalen over hoe je die zaken wilt gaan beschermen. Dat beleid moet resulteren in maatregelen. Dat kan van alles zijn; hardware maatregelen, fysieke maatregelen, software maar ook procedures waar mensen zich aan moeten houden. Dat geheel moet ervoor zorgden dat security wordt gewaarborgd. Daarnaast is ook een essentieel onderdeel dat zaken worden gelogd en dat er bijgehouden wordt bijvoorbeeld wie waarbij komt, met name als het gaat om kritische data en dat die ook logisch en regelmatig worden bekeken. Dat je dus achteraf ook security incidenten kan detecteren. Dat zijn vrij basale zaken die aan de basis liggen voor een goede security.
SP1: Ik was eigenlijk iets te ver op de zaken voor uit gelopen zag ik. Ik wilde deze vraag iets later stellen. Ik heb nog een paar andere vragen die eerst moeten. Heeft u enig idee hoe ver de ontwikkelingen zijn op het gebied van Smartapparatuur en kunt u dat onder woorden brengen?

SP2: Ja, waarschijnlijk heb ik daar een redelijk beeld van. Er zijn eigen huis apparatuur die je als smart kan bestempelen, denk bijvoorbeeld aan een smart-tv. Daarnaast lees ik ook literatuur waar ook smartapparatuur zeer actueel is en de aandacht opstrijkt.
SP1: Komt u zelf op school bijvoorbeeld ook veel Smartapparatuur tegen?
SP2: De Open Universiteit is een school waar men niet fysiek aanwezig is. Het is een school op afstand dus dat is een andere setting. In Nijmegen is het een ander verhaal, maar daar wordt nog niet met veel smartapparatuur gewerkt. Het is daar nog meer het klassieke bord met krijt of een PowerPointpresentatie maar geen smartbord of iets dergelijks.
SP1: Heeft u wel enig idee welk soort smartapparatuur er wel wordt gebruikt binnen organisaties? Heeft u daar een idee over? Met name in de zorgsector of anders algemeen.
SP2: Alle Smartapparatuur die je op dit moment kan aanschaffen daar is een deel van gericht op de consumermarkt (de mensen thuis) maar die apparaten vindt je ook in toenemende mate binnen bedrijven en organisaties. Die consumer producten vindt je daar ook terug. Dat vormt een bedrijfsrisico qua security. Veel van die smartapparaten is de security niet mee ontworpen.
SP1: Wat bedoelt u daar precies mee?
SP2: Er is in sommige devices überhaupt geen security te bespeuren. Bij andere devices zijn er wel securitymaatregelen genomen, maar daar zitten manco's aan. Neem bijvoorbeeld een apparaat waartoe toegang is geregeld met een wachtwoord, maar het is een default wachtwoord wat makkelijk te raden is en algemeen bekend is. Het is moeilijk om dat wachtwoord aan te passen, of het kan alleen maar als je de firmware aanpast. Er zitten wel securitymaatregelen in, maar in de praktijk zijn die makkelijk te omzeilen. Hierdoor is er niet echt sprake van beveiliging.
Sp1: Verschilt dit per producent?
Sp2: Dat zou ik niet zo durven zeggen. Ik denk dat het verschilt per product en waar die voor bedoeld is. In de consumermarkt wordt er minder zwaar aan beveiliging getild, dan bij apparaten die in kritische infrastructuur worden gebruikt. Bij de apparaten die daarvoor bedoeld zijn, zijn zwaardere securitymaatregelen genomen.
SP1: Hoe bekend zijn organisaties met Smartapparatuur? En heeft u enig idee hoe bekend de zorgsector?
SP2: Een organisatie is een verzameling van werknemers in die organisatie. Er is vrijwel niemand meer tegenwoordig die nooit heeft gehoord, of heeft gewerkt met een smart apparaat. Als ik een telefoon ook als een smart app beschouw. Iedereen heeft er in een organisatie notie en kennis van.
Sp1: Hoe staat het met de beveiliging van smartapparatuur?
Sp2: De beveiliging is nog niet optimaal omdat ze dus gericht zijn op de consumer market
Sp1: Zijn organisaties zich bewust van risico's van smartapparatuur? Ik denk dat ze zich nog te weinig bewust zijn.
Sp2: Welke risico's zijn er bij het gebruik van smartapparatuur?

Bijlage IV Transcript interview Mariëlle Stoelinga

Sp1: Bij deze ben ik begonnen, zal ik nog even toelichten waar het over gaat?
Sp2: Ja
Sp1: Ik doe mijn afstudeeropdracht voor de opleiding integrale veiligheidskunde en mijn afstudeerrichting is smartapparatuur. Ik onderzoek met name in de zorgsector, welke risico's er spelen en hoe ik het bedrijf waar ik stage loop, advies kan geven over dit onderwerp. Het stagebedrijf waar ik stageloop is een informatiebeveiligingsbureau genaamd Sincerus.
Sp2: Oké
Sp1: Ik onderzoek dus met name eerst wat de rol is van smartapparatuur in de zorgsector. Hoeveel wordt er gebruik van gemaakt. Daarvoor ben ik bij verschillende ziekenhuizen en zorginstellingen langs geweest. Daarnaast kijk ik naar de risico's en als laatste kijk ik naar maatregelen die getroffen kunnen worden en uiteindelijk moet er een soort van adviesproduct uitrollen waarmee ze advies kunnen geven over dit onderwerp.
Sp2: Uhu.
Sp1: Ik heb een eigen definitie gehanteerd van smartapparatuur omdat overal in de literatuur andere termen worden gebruikt. Deze definitie is; 'Smartapparatuur zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kan uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kan zijn op een intern netwerk en met elkaar kunnen communiceren.'
Sp2: Oké.
Sp1: het is de wens van de opdrachtgever geweest om telefoons, computers en tablets niet mee te nemen maar om me echt te richten op de nieuwe generatie smartapparatuur. Deze huishoudelijke apparaten die gaan van de consumentenmarkt steeds meer naar de zakelijke markt. Misschien kunt u wat vertellen over uw achtergrond? Ik weet dat u toevallig ook onderzoek doet naar dit soort dingen heb ik gelezen. Of gaat doen in ieder geval.
Sp2: Ja, wat is mijn achtergrond? Ik ben Universitair hoofddocent en mijn vakgebied is risicomanagement van hightechsystemen en ik kijk zowel naar safety risico's als naar security risico's. Ik kijk dus zowel naar het ontstaan van risico's door fouten, als naar het ontstaan van risico's door echte aanvallen. Echt bedoelde aanvallen. Ik kijk vooral naar methoden om die goed in kaart te brengen om onafhankelijkheden tussen die risico's te moduleren en ook te analyseren. Dan moet je maatregelen treffen en moet je kijken wat het effect is van die maatregelen. Wat voor soort risicoreductie heb je.
Sp1: Kunt u wat vertellen over uw onderzoek die u doet of die u in de toekomst nog gaat doen?
Sp2: Ik doe veel foutboomanalyses, dat is safety en attack. Dat is meer security via een aanvalsboom. Ik kijk vooral naar hoe kan ik al die aanvalspaden zo goed mogelijk in kaart brengen.
Sp1: Het klopt wel dat u onderzoek gaat doen naar Internet of Things toepassingen?
Sp2: Ja, met name in ziekenhuizen, dus dat heeft wel raakvlakken. We zijn er mee bezig maar we zijn echt bezig met de eerste opzet. Wat we daar vooral gaan doen is kijken of het aansluit bij stakeholders, want je kunt alles technisch alles nog zo veilig ontwerpen. Als het niet veilig ingekaderd is in de context, de gebruikerscontext, dan werkt het gewoon niet. Als het wachtwoord met een post-it op de computer wordt gehangen, dan kan alles alsnog zo goed beveiligd zijn maar dan werkt het niet. Dus het is heel erg het samenspel tussen menselijke en technische factoren.
Sp1: Hoe bekend bent u zelf met smartapparatuur?
Sp2: Ik ben bekend met de trends daarvan, maar ik heb nog nooit zelf een definitie daarvan gezien, maar ik heb er natuurlijk wel een beeld bij.
Sp1: U weet ervan? U weet wat het zijn?
Sp2: Jazeker, smart is een van de Buzz-words.
Sp1: Hoe zorg je ervoor dat de informatie goed is afgesteld op de kritische processen van de organisatie?
Sp2: Dat is een hele grote vraag, daar kun je hele proefschriften over volschrijven. Ik wil daar best iets over zeggen, maar dat is een ontzettend brede vraag waar heel veel deelaspecten een rol spelen en wat meerdere jaren onderzoek van een vakgroep zou kunnen zijn.
Sp1: Als het een heel breed antwoord is dan slaan we deze eerst over en kunnen later kijken of we nog tijd hebben. Heeft u enig idee hoe ver de ontwikkelingen van smartapparatuur op dit moment is?

Sp2: Ver, alles is smart. Als het nog niet op de markt is, dan komt het er heel snel aan. Je kunt het zo gek niet bedenken. Ik las laatst iets over vibrators die je aan het internet kan hangen. Daar heb ik nog niet eens aan gedacht. Was niet in mij opgekomen. Als dat al smart is, wat is dan niet smart?
Sp1: Alles is mogelijk dus tegenwoordig. Weet u ook hoe bekend organisaties met smartapparatuur zijn, met name in de zorgsector?
Sp2: Ik denk dat de zorgsector weet dat het bestaat, maar erg huiverig is om het in te voeren. Invoeren in een organisatie is niet zo gemakkelijk. Thuis koop je gewoon een smartthermostaat en ben je klaar. In een ziekenhuis moet de gehele organisatie zich richten op die smartprocessen. Die moeten heel goed ingebed worden in de hele workflow van een organisatie. Er zijn allerlei protocollen, want een ziekenhuis is ontzettend geprotocolleerd. Als je iets 'smarts' wil doen moet je kijken of de protocollen nog voldoende zijn, adequaat zijn, of dat er veranderingen in moet komen. Er moet over nagedacht worden, het moet goedgekeurd worden en iedereen moet er zijn zegje over doen.
Sp1: Het is niet een kwestie van even kopen en toepassen, maar je moet je hele organisatiestructuur erop aanpassen.
Sp2: Ja en aan de andere kant zie ik ook; ik weet niet specifiek over ziekenhuizen maar je ziet bijvoorbeeld bij de politie, dat politieagenten zelf dingen met de mobiel gaan doen in plaats van met handheld devices die ze van werk krijgen. Dit komt doordat hun eigen mobieltjes een bepaalde functionaliteit hebben die die andere apparaten niet hebben. Zo fietsen ze om de richtlijnen heen en daar kun je van alles van vinden, dit brengt risico's met zich mee maar brengt ook praktische voordelen. Hier blijkt wildgroei te ontstaan.
Sp1: Heeft u een beeld bij welke smartapparatuur er worden gebruikt binnen de zorgsector?
Sp2: Ja, als je het niet over iPads hebt en dergelijke. Ziekenhuizen hebben een eigen intern netwerk om medische gegevens uit te wisselen tussen afdelingen en administratie. Maar is dat smart? Telemetrie is erg in opkomst. Dat communicatie veel meer via wireless gaat dan via bedrade netwerken. Sommige huisartsen doen het wel. Heb je een moedervlek die er raar uit ziet, dan stuur je een appje naar je huisarts die er even naar kijkt. Huisartsen doen dit op hun eigen telefoon. Dit is een typisch voorbeeld dat het buiten de workflow omgaat.
Sp1: Je had het over het interne netwerk. Ik schaar alles wat aan het interne netwerk is gekoppeld onder smartapparatuur.
Sp2: Gewoon al die CT-scans, MRI-scans.
Sp1: Er zijn er wel heel veel. Maar ik heb van een geïnterviewde gehoord dat er in een ziekenhuis bijna niet gebruik van gemaakt wordt. Het kan natuurlijk zo zijn dat hij een verkeerd beeld heeft.
Sp2: Als jij dat zegt met jouw definitie van smart, dan zijn echoapparatuur gewoon smart.
Sp1: Niet alle medische apparatuur staan in verbinding met het internet denk ik?
Sp2: Dat weet ik niet helemaal precies. Maar ik vermoed dat als die echobeelden, longfoto's of hartfilmpjes worden beschouwd door de arts dat dat over het internet of het interne netwerk gaat.
Sp1: Ja precies maar is het de foto die over het internet gaat of is gaat het hier om het apparaat die de foto maakt? Ik heb het echt over objecten en apparaten die afzonderlijk IP-adressen hebben en kunnen opereren als een soort computer.
Sp2: Een eigen proces en units dus.
Sp1: Voorbeelden zijn onder andere Smart-tv, slimme koelkast of slimme stofzuigers.
Sp2: Oké, ja.
Sp1: Hoe staat het eigenlijk met de beveiliging van Smartapparatuur?
Sp2: De common opinion is, dat ze zo lek zijn als een mandje.
Sp1: Oké, en waar blijkt dat uit?
Sp2: Onder andere aan de kosten en time-to-market. Het is duur om IoT-devices goed te beveiligen en het vereist expertise om dat te doen. Als jij de eerste bent die met een eerste funky smart-vibrator op de markt komt dan kun je er veel verkopen. Als je de tweede bent dan verkoop je minder en is het minder funky. Er is heel veel druk om een korte 'time-to-market' te hebben en als eerste een product op de markt te brengen. Er is gewoon geen tijd voor securityreviews en gedegen beveiliging. Wat mensen gaan doen is het volgende; ze nemen een oud device, ze stoppen er wat sensoren in, stoppen er een marketingsausje overheen en klaar. Dat is natuurlijk heel wat anders dan wat je moet doen om het allemaal beveiligd te krijgen.
Sp1: Dus dat ligt heel erg bij de producent van die producten?

Sp2: Ja, bij home-appliances wel. Daar heb je ook te maken met dat de routers niet goed beveiligd zijn.
Sp1: Is het ook een risico dat de producten voornamelijk voor de consumentenmarkt worden gemaakt en niet voor de zakelijke markt?
Sp2: Phising is ook een risico. Nog wel meer bij de consumentenmarkt dan bij de zakelijke markt. Zakelijke markt, ja dat mag je hopen.
Sp1: Ik heb wel ergens gelezen dat als je, je op de consumentenmarkt richt dat een producent het product zo op de markt kan gooien. Als een producent zich op de zakelijk markt wil richten komen er natuurlijk veel meer dingen bij kijken.
Sp2: Het management van ziekenhuizen zijn vaak medisch geschoolde mensen, die de meeste affiniteit hebben met waar hun core-expertise ligt. Daar ligt het ook aan.
Sp1: Ze weten er niet genoeg van af?
Sp2: Dat is niet erg, want ze kunnen mensen aannemen die er wel verstand van hebben. Alleen zijn ze er dan wel van doordrongen hoe ernstig dit is?
Sp1: Welke risico's spelen er eigenlijk bij het gebruik van smartapparatuur?
Sp2: Net zoals bij andere beveiligingsrisico's. Het eerste is patiëntdata, privacy van de patiënten. Natuurlijk ook uitval van de systemen. Je kunt makkelijk een ziekenhuis plat leggen. Het nare van Internet of Things, er zijn zoveel ingangen op het internet. Je hoeft maar één ingang te hebben en dan kan je via het ene device naar het andere device, totdat je bij allerlei kritische systemen kunt komen.
Sp1: Welke vormen van hacken zijn er mogelijk bij een smartapparaat?
Sp2: Je kunt het overnemen. Dat is grappig, maar daar win je de oorlog niet mee. Het is gevaarlijk als je de IoT-devices gebruikt om bij meer kritische systemen te komen.
Sp1: Je kan dus via zo'n device wel op het interne netwerk komen begrijp ik?
Sp2: Ja.
Sp1: Zijn organisaties in de zorgsector zich ook bewust van die risico's?
Sp2: In de zorgsector speelt er nog iets mee, dat is typerend voor de zorg, beschikbaarheid van data is heel belangrijk. Als een patiënt binnenkomt en het een noodgeval betreft, wil de arts meteen kunnen zien wat het medisch profiel is van de patiënt. Deze zit niet te wachten om dan nog drie wachtwoorden in te voeren.
Sp1: Dus die wil de gegevens zo snel mogelijk voor zich hebben.
Sp2: Ja, goed dat is één aspect. Wat was je vraag?
Sp1: Zijn de organisaties zich bewust van de risico's?
Sp2: Ik denk onvoldoende.
Sp1: Waar blijkt dat uit?
Sp2: Omdat ze het er nooit over hebben.
Sp1: Hoe zit het met medewerkers die er gebruik van maken?
Sp2: Het grote probleem met security is gewoon heel er onhandig. Kijk maar naar je eigen huis. Het is onhandig dat je de hele tijd je sleutel bij je moet hebben en dat wanneer je die sleutel kwijt bent, je buiten gesloten bent. Je wilt dat je ouders, man en kinderen wel binnen kunnen komen en die hebben dan weer een aparte sleutel nodig. Ze kunnen die ook weer verliezen, wat niet praktisch is. Het zou makkelijker zijn om de deur gewoon open te laten maar zo zit de wereld nou eenmaal niet in elkaar. En iedere securitymaatregel is extra lastig. Er zijn nog geen echte ongelukken gebeurd. Als je het vergelijkt met een kerncentrale zijn er concrete voorvallen geweest en is gewoon heel duidelijk. Dit moeten we niet hebben.
Sp1: Dus er zijn geen voorbeelden waar het mis is gegaan, waardoor ze de beveiliging willen aanpassen.
Sp2: Ja, dat het zo ernstig mis is gegaan.
Sp1: Wie moeten ervoor zorgen dat ze het wel gaan doen? Moeten ze dat zelf doen of moet dat vanuit de overheid geregeld worden?
Sp2: Dat is een debat dat je kunt hebben. Wat meer sturing van bovenaf ben ik niet op tegen. De vliegtuigindustrie wordt vaak aangehaald als een voorbeeld waar het goed geregeld is. Als jij je vliegtuigsafety niet op orde hebt, dan krijg je gewoon geen landingsrechten.
Sp1: Zulke dingen zou je ook in de ziekenhuiswereld moeten invoeren?
Sp2: Ja.
Sp1: Welke maatregelen moet een organisatie treffen zodat de kritische processen geen gevaar lopen bij het gebruik van smartapparatuur?

Sp2: Een hele brede vraag en ik denk dat het antwoord niets anders is dan het antwoord op niet smartapparatuur. Je hebt organisatorische maatregelen, technische maatregelen en psychologische maatregelen. Ik zou eerst denken, stel een chief security officer aan. Maak één iemand verantwoordelijk voor de security van ziekenhuizen.
Sp1: Die zijn er al wel toch?
Sp2: Dingen die in de industrie volstrekt normaal zijn, vind ik bij ziekenhuizen altijd tegenvallen. Ik heb geen harde cijfers, maar ik denk dat er nog wel ruimte voor verbetering in zit.
Sp1: Stel je voor dat er wel zo'n chief security officer aanwezig is, waar moet deze op letten voordat hij smartapparatuur in gebruik gaat nemen? Waar moet de apparatuur op getoetst worden, ook wanneer het aan het interne netwerk wordt gehangen?
Sp2: Er is een risicomanagementcyclus voor security. Er zijn allemaal ISO-standaarden voor hoe je het moet aanpakken. Haal de juiste stakeholders bij elkaar, schat de risico's in op impact en likleyhood en identificeer maatregelen. Evalueer en monitor dit continu.
Sp1: Dus eigenlijk verschilt dit niet veel van andere cyberrisico's?
Sp2: Nee, alleen uit de risicoanalyse zullen andere factoren naar boven komen dan in een kerncentrale.
Sp1: Zou je dus niet iets anders moeten aanpakken voor smartapparatuur omdat deze in opkomst zijn en dus minder goed beveiligd zijn?
Sp2: Nee, technische maatregelen zijn belangrijk maar ook organisatorische maatregelen. Het is belangrijk dat het risicomanagementcyclus goed is ingebed in het bedrijfsproces, dat daar op gemonitord wordt en jaarlijks gereviewd wordt.
Sp1: Wat zijn de beweegredenen van een crimineel om in de zorgsector een aanval uit te voeren en waarom zouden ze dat via smartapparatuur willen doen?
Sp2: Voor dat laatste verschilt het in de zorgsector niet zoveel van de situaties in andere domeinen. En ook smartapparatuur verschilt niet veel van niet smartapparatuur. Wat er natuurlijk wel is; smartapparatuur is nieuw. Er zitten meer veiligheidslekken, als je echt een Internet of Things hebt, dan zijn er veel entrypoints. Maar je kunt de normale aanvallersprofielen bekijken en die ken je waarschijnlijk. Je hebt bijvoorbeeld overheden, criminelen en scriptkiddies. Die hebben allemaal te maken met skills, resources, incentives en risk appetite. Dat kan je hier ook op toepassen.
Sp1: Daar zit geen verschil in dus? Eigenlijk is het allemaal hetzelfde maar doordat deze apparaten nieuw zijn en is het makkelijk te gebruiken. Het is de weg van de minste weerstand op dit moment?
Sp2: Ja, en het is ook dat ziekenhuizen zelf een hele complexe organisatiestructuur met maatschappen. Dat maakt het niet makkelijk. Ze hebben ook een hele andere safetycultuur. Bij bijvoorbeeld defensie en de vliegtuigindustrie is er meer bereidheid om regels na te leven. Misschien is heeft het ook te maken met de werkdruk of de hoeveelheid.
Sp1: Hoe effectief zou een bewustwordingstraining zijn op het gebied van smartapparatuur. Hoe je daar mee om moet gaan of bewust maken van de risico's?
Sp2: Als een training gaat om zenden dan geloof ik er niet zo in. Als je een security awareness cultuur wil creëren dan moet je dat met co-creatie doen. De werkvloer moet je bij het proces betrekken. Wij willen hier minder ongeluk of het nou om safety of security ongelukken gaat maakt niet uit. Hoe gaan we dat organiseren met z'n allen.
Sp1: Wat bedoelt u dan met co-creatie?
Sp2: Dat niet het management moet zeggen: 'we gaan een training doen' of 'we gaan deze maatregelen opleggen zoals je handen wassen voor je met patiënten gaat werken.' Als je dat van bovenaf oplegt, dan is er minder bereidheid om die regels na te leven. Co-creatie is ook een buzzword. Je betrekt alle stakeholders bij een probleem. Patiënten, verplegend personeel, artsen maar ook de logistieke kant van het ziekenhuis.
Sp1: Oké, heeft u nog even tijd?
Sp2: Ja hoor nog vijf minuten.
Sp1: Is het een zwakte dat standaardwachtwoorden niet worden veranderd van smartapparatuur?
Sp2: Jazeker, dat is ook zo bij routers.
Sp1: Ligt dat aan de producenten of ligt dat aan de gebruikers?
Sp2: Allebei natuurlijk. Producenten kunnen daar iets aan doen natuurlijk. Als je een telefoon koopt dan krijg je wel een puck code die je erbij krijgt.

Sp1: Daar is wel wat te halen voor een organisatie om ervoor te zorgen dat die standaardwachtwoorden altijd worden veranderd?
Sp2: Ja, wachtwoordmanagement in het algemeen is bijvoorbeeld een van de technische maatregelen die je kunt nemen. Dat is dat mensen ieder jaar hun wachtwoord updaten en dat ze misschien minder wachtwoorden nodig hebben.
Sp1: Is het van belang dat er beleid komt, wie er bij die smartapparatuur kan komen?
Sp2: Ja, acces control is net weer een voorbeeld van een van die andere maatregelen die je kan nemen. Je moet er ook voor zorgen dat als mensen uit dienst gaan van een organisatie dat ze hun credentials kwijtraken.
Sp1: Dat zijn dus eigenlijk standaard maatregelen die overal in die informatiebeveiliging worden toegepast?
Sp2: Ja.
Sp1: Die komen uit de normen?
Sp2: Die normen die zeggen; breng risico's in kaart, die geven niet een soort checklist van dit zijn typische risico's.
Sp1: Hoe komt u aan die maatregelen? Waar kan ik dat vinden?
Sp2: Dat staat in boeken over information security.
Sp1: Daarom heb je ook experts nodig. Netwerkbeveiliging is weer wat anders, dan zorgen voor die sociale cultuur. Physical acces.
Sp1: Je moet smartapparatuur moet je dus eigenlijk scharen onder de algemene informatiebeveiliging en de algemene maatregelen erop toe passen. Je hoeft dus geen aparte maatregelen te hanteren?
Sp2: In de technische maatregelen zitten er wel verschillen. Bijvoorbeeld met die standaardwachtwoorden. Als je normale informatiebeveiliging toepast, dan zie je in de technische details natuurlijk wel verschil. Het maakt uit of je voor een selfdriving car-maatregelen neemt of bij een CT-Scanner. Hoe dat technisch werkt, maakt wel uit.
Sp1: Het grootste risico is dus dat het een nieuw product betreft en de beveiliging nog niet optimaal is en daardoor kunnen mensen via die manier binnen komen. Eigenlijk als je een tijdje verder bent, is dit niet meer aan de orde?
Sp2: Nou, er moet wel wat gebeuren. Er moeten hierboven zich wel mensen druk over gaan maken. Als iedereen denkt; het loopt wel los en over vijf jaar is het probleem vanzelf opgelost. Dat is niet zo. Dan kunnen er wel echt ongelukken gebeuren.
Sp1: Als er echt iets gebeurd dan gaat het pas rollen denk ik?
Sp2: Ja, er zijn wel wat security incidenten geweest met creditcards DDoS-aanvallen.
Sp1: Dan is het nog maar heel kort natuurlijk een site die even platligt? Dan heb je alleen maar reputatieschade en economische schade. Nog nooit is er bij zo'n ziekenhuis iets met patiënten gebeurd op deze manier?
Sp2: Ja, maar dat weten we ook niet. Er wordt natuurlijk ook veel, net als bij banken, geheimgehouden.
Sp1: Is het de toekomst dat alles smart wordt? Hoe snel zou dat gaan?
Sp2: Ik denk het wel en ik verwacht dat we over vijf jaar een stuk verder zijn met smart.
Sp1: Is dat een goed iets of is dat een groot risico?
Sp2: Dat is het denk ik allebei.
Sp1: De gebruikersgemakken moeten hoger wegen dan de risico's?
Sp2: Risico's zijn zeldzaam, ze hebben wel een hoge impact en het gemak is groot. Het is dus erg verleidelijk om te denken dat niet ik, maar mijn buurman wordt aangevallen.
Sp1: Is het dan wel goed voor een ziekenhuis om die apparatuur nu te nemen, nu het nog niet goed beveiligd is?
Sp2: Ik zal die apparatuur alleen maar nemen als het wel goed beveiligd is. Het is sowieso een goed idee om het hele ziekenhuis te beveiligen.
Sp1: Ze moeten sowieso dus nog een hele slag slaan?
Sp2: Ja.
Sp1: Dan wil ik het gezien de tijd hier wel bij laten. Ik had nog iets meer vragen maar we hebben het meeste wel gehad.
Sp2: Welke vragen had je nog dan?
Sp1: Welke vormen van hacken zijn er mogelijk via smartapparatuur?

Sp2: Alle vormen die normaal ook kunnen.
Sp1: Samenvattend, wat zijn de belangrijkste risico's?
Sp2: Patiënt privacy, en het platleggen van systemen. De maatregelen zijn: implementeer de normale informatiebeveiligingscylcus. Stap 1 is stel iemand verantwoordelijk voor het implementeren van het standaard risicocyclus. Daar horen organisatorische en technische maatregelen bij. Beide zijn belangrijk. Co-creatie is een organisatorische maatregel om ervoor te zorgden dat beleid ook wordt uitgevoerd.
Sp1: De co-creatie is dus heel belangrijk?
Sp2: Ja, als je mensen niet laat meedenken dan gaan ze tegen denken. Dat is regel nummer één. Al die dingen die je noemt; acces control, wachtwoordmanagement, goed personeelsbeleid, als mensen de organisatie verlaten dat sleutels niet meer werken en awareness trainingen, dat zijn de normale security dingen. Je moet hier gewoon extra scherp in zijn, maar er zijn geen nieuwe maatregelen te bedenken.
Sp1: Misschien kan het zo zijn dat je ze niet aan kritische processen moet hangen omdat deze apparaten nog heel kwetsbaar zijn?
Sp2: Zeker, ik weet bijvoorbeeld dat Rijkswaterstaat allerlei tunnels niet aan het internet hangt omdat het nu werkt. Het is onhandig dat je daar heen moet rijden als je iets moet fixen. Geen IoT hebben is ook een maatregel.
Sp1: Nu moet ik er vandoor.
Sp2: Hartelijk bedankt voor uw informatie en tijd.
Sp1: Graag gedaan.

Bijlage V Transcript interview Stephan Hazekamp St. Jansdal

SP1: ‘Smartapparaten zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kunnen zijn op een intern netwerk en met elkaar kunnen communiceren.’ Bent u bekend met de term ‘Smartapparatuur’?
Sp2: Ja.
Sp1: Hoe bekend is uw organisatie met Smartapparatuur?
Sp2: Minder bekend. De Smart health staat in de kinderschoenen. Je moet wel een visie hebben bij het invoeren. Het moet worden ingevoerd om de zorg beter te maken.
Sp1: Welke van de volgende apparaten zijn er aanwezig in uw gebouwen en in welke hoeveelheid?
Sp1: Slimme thermostaat?
Sp2: Ja.
Sp1: Slimme verlichting?
Sp2: Ja.
Sp1: Slimme lampen?
Sp2: Ja.
Sp1: Slimme Koelkast?
Sp2: Nee.
Sp1: Wifi Koelkast?
Sp2: Nee.
Sp1: Slimme wasmachine?
Sp2: Nee.
Sp1: Slimme droger?
Sp2: Nee.
Sp1: Slimme stofzuiger?
Sp2: Nee.
Sp1: Robot Stofzuiger?
Sp2: Nee.
Sp1: Slimme deurbel?
Sp2: Nee.
Sp1: Smart-tv?
Sp2: Ja, een stuk of 20.
Sp1: Slimme sloten?
Sp2: Nee.
Sp1: Smart alarm?
Sp2: Nee.
Sp1: Slimme tas?
Sp2: Nee.
Sp1: Smartwatch?
Sp2: Alleen voor eigen gebruik, maar geen zicht op.
Sp1: Slimme stekkers?
Sp2: Nee.
Sp1: Slimme horloges?
Sp2: Nee.
Sp1: Slimme koffiemachines?
Sp2: Nee.
Sp1: Slimme meters?

Sp2: Nee.
Sp1: IoT-sensoren?
Sp2: Nee.
Sp1: Smart health?
Sp2: Ja, zo'n 20-30% van de medische apparatuur is smart. Onder ander pacemakers en Cd-magneten.
Sp1: Anders namelijk?
Sp2: Nee.
Sp1: Heeft u zicht op de smartapparatuur die gebruikt wordt door medewerkers?
Sp2: Nee.
Sp1: Welke apparaten worden het meest gebruikt en staan deze constant in verbinding met het bedrijfsnetwerk?
Sp2: Smart Health.
Sp1: Heeft u overzicht over alle apparaten die in verbinding staan met het bedrijfsnetwerk?
Sp2: Er is een overzicht aanwezig.
Sp1: Waar let u op bij de aanschaf van smartapparatuur?
Sp2: Er wordt een risicoanalyse uitgevoerd op nieuwe apparaten. Er wordt onder andere gekeken of de maatregelen beheersbaar zijn. Daarnaast wordt er naar de privacy van de patiënten gekeken.
Sp1: Heeft u een checkprocedure voordat de smartapparatuur het netwerk op gaan?
Sp2: De ICT-afdeling heeft checklijsten die worden afgehandeld voor een apparaat het internet op mag.
Sp1: Verandert u de standaard wachtwoorden van de smartapparatuur?
Sp2: Daar heb ik geen zicht op.
Sp1: Heeft u zicht op risico's van deze apparaten?
Sp2: Op sommige vlakken wel. Er zijn standaard risico's die erg voor de hand liggen. Deze risico's ken ik wel.
Sp1: Wat doet u als internetsystemen niet meer werken?
Sp2: Opschalen, Het is dan een crisissituatie. Er zijn wel back-ups beschikbaar.
Sp1: Waarom zou uw organisatie slachtoffer kunnen worden van cybercriminaliteit?
Sp2: Financieel gewin. Ik zou niet me niet kunnen voorstellen dat iemand via deze manier slachtoffers wil maken. De hacktechnologie zal wel vorderen dat ze het kunnen maar ik zou niet inzien waarom ze dat zullen doen. Het kan natuurlijk wel reputatie en imagoschade geven aan een ziekenhuis als er gegevens lekken of iets dergelijks. Het lastige is ook dat de technologie eerst komt en dan pas de veiligheid.
Sp1: Is er een business continuity plan aanwezig en kunt u daar wat over vertellen?
Sp2: Er is een business continuity plan aanwezig en deze zorgt ervoor dat de processen zo snel mogelijk weer draaien.
Sp1: Hoe is de informatiebeveiliging afgesteld op de kritische processen?
Sp2: Het informatiemanagementsysteem moet op een bepaald niveau blijven en deze moet worden blijven opgebouwd en je moet het telkens aanpassen aan de nieuwste wet en regelgeving.
Sp1: Volgens VMS zorg is het de bedoeling dat de patiëntveiligheid wordt gewaarborgd en de onbedoeld vermijdbare schade in ziekenhuizen terug wordt gedrongen door het verbeteren van deze thema's. Patiënten lopen risico doordat onder andere patiëntgegevens, medicijngebruik en voedselaanbod vaak digitaal wordt geregeld. Als cybercriminelen via smartapparatuur het bedrijfsnetwerk in kunnen komen en bij deze gegevens kunnen dan is er een kans dat deze gegevens worden aangepast of versleuteld waardoor een patiënt de verkeerde voeding of medicijnen krijgt. Dit kan uiteindelijk levens kosten. Als patiëntgegevens niet kloppen of er niet meer zijn dan kan er verkeerde zorg worden verleend wat een dodelijke afloop kan hebben. Welke maatregelen zouden er getroffen moeten worden om dit tegen te gaan?
Sp2: Hoog niveau informatiebeveiliging is belangrijk alleen blijf je altijd achter de hack ontwikkeling aanlopen. De nieuwste beveiliging komt pas als er een incident is geweest.

Bijlage VI Interview Jeroen Geerdink Ziekenhuisgroep Twente

Smartapparatuur

'Smartapparaten zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kunnen uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kunnen zijn op een intern netwerk en met elkaar kunnen communiceren.'

Sp1: Bent u bekend met de term 'Smartapparatuur'?
Sp2: Ja.
Sp1: Hoe bekend is uw organisatie met Smartapparatuur?
Sp2: Redelijk goed.
Sp1: Welke van de volgende apparaten zijn er aanwezig in uw gebouwen en in welke hoeveelheid?
Sp1: Slimme thermostaat?
Sp2: Ja.
Sp1: Slimme verlichting?
Sp2: Ja, op ic.
SP1: Slimme lampen?
Sp2: Ja.
Sp1: Slimme koelkast?
Sp2: Ja, medische koelkasten met sensors.
Sp1: Wifi Koelkast?
Sp2: nee.
Sp1: Slimme wasmachine?
Sp2: Ja, bij centrale sterilisatie.
Sp1: Slimme droger?
Sp2: Nee.
Sp1: Slimme stofzuiger?
Sp2: Nee.
Sp1: Robot stofzuiger?
Sp2: Nee.
Sp1: Slimme deurbel?
Sp2: Nee.
Sp1: Smart-tv?
Sp2: Ja.
Sp1: Slimme sloten?
Sp2: Ja.
Sp1: Smart alarm, De smart alarm is een alarm die veel meer kan dan alleen maar beveiligen, de smart alarm is een alarm die meldingen doorstuurt naar uw telefoon of smartwatch?
Sp2: Ja.
Sp1: Slimme tas?
Sp2: Nee.
Sp1: Smartwatch?
Sp2: Ja.
Sp1: Slimme Stekkers?
Sp2: Nee.
Sp1: Slimme horloges?
Sp2: Nee.
Sp1: Slimme koffiemachines?
Sp2: Nee.
Sp1: Slimme meters?
Sp2: Ja.
Sp1: IoT-sensoren zoals temperatuur sensoren bewegingssensoren etc.?

Sp2: Ja.
Sp1: Smart Health: Medische apparatuur zoals pacemakers en insulinepompen?
Sp2: Ja.
Sp1: Oproepsysteem zorg (voorheen pieper)
Sp2: Ja.
Sp1: Anders namelijk?
Sp2: Liften, deuren, ventilatoren besturing/monitoring via gebouwbeheerssysteem, infusie apparatuur, voedingspompen.
Sp1: Heeft u zicht op de smartapparatuur die gebruikt wordt door medewerkers?
Sp2: Nee, geen verantwoordelijkheid vanuit mijn functie in deze.
Sp1: Welke apparaten worden het meest gebruikt en staan deze constant in verbinding met het bedrijfsnetwerk?
Sp2: Vrijwel alle genoemde apparatuur.
Sp1: Heeft u overzicht over alle apparaten die in verbinding staan met het bedrijfsnetwerk?
Sp2: ICT-netwerkbeheer heeft overzicht van alle aangesloten apparatuur.
Sp1: Waar let uw organisatie op bij de aanschaf van smartapparatuur?
Sp2: Patiëntveiligheid, security (privacy) en diverse normeringen. De inpassing in ICT-landschap van ZGT.
Sp1: Is er een checkprocedure voordat de smartapparatuur het netwerk op gaan?
Sp2: Ja.
Sp1: Veranderen jullie standaard wachtwoorden van de smartapparatuur?
Sp2: Weet dit niet zeker, maar denk van niet.
Sp1: Heeft u zicht op risico's van deze apparaten?
Sp2: Er wordt altijd een risicoanalyse uitgevoerd. Zie de QMT-aanpak.
Sp1: Wat doen jullie als internetsystemen niet meer werken?
Sp2: Noodprocedure afhankelijk van proces of type systeem.
Sp1: Hebben jullie enig beleid wat betreft deze apparatuur?
Sp2: Indien het een kritisch systeem is voor het proces is er altijd een noodprocedure aanwezig.
Sp1: Waarom zou uw organisatie slachtoffer kunnen worden van cybercriminaliteit?
Sp2: Omdat beveiliging nooit volledig 100% is.
Sp1: Is er een business continuity plan aanwezig en kunt u daar wat over vertellen?
Sp2: Ja, verschillende. Deze zijn procesafhankelijk.
Sp1: Hoe is de informatiebeveiliging afgesteld op de kritische processen?
Sp2: Conform NEN7510/12/13
Sp1: Volgens VMS zorg is het de bedoeling dat de patiëntveiligheid wordt gewaarborgd en de onbedoeld vermijdbare schade in ziekenhuizen terug wordt gedrongen door het verbeteren van bepaalde thema's. Patiënten lopen risico doordat onder andere patiëntgegevens, medicijngebruik en voedselaanbod vaak digitaal wordt geregeld. Als cybercriminelen via smartapparatuur het bedrijfsnetwerk in kunnen komen en bij deze gegevens kunnen dan is er een kans dat deze gegevens worden aangepast of versleuteld waardoor een patiënt de verkeerde voeding of medicijnen krijgt. Dit kan uiteindelijk levens kosten. Als patiëntgegevens niet kloppen of er niet meer zijn dan kan er verkeerde zorg worden verleend wat een dodelijke afloop kan hebben. Welke maatregelen zouden er getroffen moeten worden om dit tegen te gaan?
Sp2: Technische en organisatorisch maatregelen conform vigerende richtlijnen NEN 7510/12/13, convenant medische hulpmiddelen en ons eigen QMT-beleid.
Sp1: Op welke manier zouden smartapparatuur invloed kunnen hebben op kritische processen?
Sp2: Voorbeeld diagnostisch proces. Meetapparatuur: Data integrity failure – foute meetwaarden – op basis hiervan verkeerd patiënt beleid (bijv.: medicatie) – resulterend in schade bij patiënt.
Voorbeeld behandel proces: Infusiepomp: Instellingen pomp remote gewijzigd- dosering foutief – resulterend in schade bij patiënt.

Bijlage VII Interviewverslag Niels Drieënhuizen Lindenhout

Smartapparatuur

'Smartapparatuur zijn elektronische apparaten en objecten die in meer of mindere mate programmacodes kan uitvoeren, met uitzondering van computers, mobiele telefoons en tablets, die aangesloten kan zijn op een intern netwerk en met elkaar kunnen communiceren.'

Niels Drieënhuizen is bekend met de term 'Smartapparatuur' zoals hier is genoemd. De medewerkers van Lindenhout weten dat het bestaat, maar verder wordt er niet veel mee gewerkt. Er wordt bij Lindenhout niet veel gebruik gemaakt van Smartapparatuur. De enige smartapparatuur die gebruikt worden zijn een paar smartwatches voor eigen gebruik. Daarnaast is er voor de rest maar één Smart-tv aanwezig op kantoor. Voor de rest heeft de jeugdzorg niet veel te maken met kritische zorg waar apparatuur wordt gebruikt. Smart health wordt in deze organisatie dus niet gebruikt. De rol van de smartapparatuur in deze organisatie kan worden omgeschreven als nihil. Er is inzichtelijk te maken welke apparaten er op het interne netwerk zijn aangesloten maar Niels Drieënhuizen weet niet welke apparaten er allemaal worden gebruikt door de medewerkers. Ze hebben nog geen ervaring met het veranderen van standaard wachtwoorden van smartapparatuur, omdat ze er dus bijna geen gebruik van maken. Er zijn back-ups aanwezig van patiëntendossiers en deze zitten op een aparte lijn. Verder heeft de organisatie niet veel ervaring met smartapparatuur.

Bijlage VIII Codeerschema's

A. Open Coderen

Code	Onderzoeksvraag	Interview
Bekendheid smartapparatuur - Organisatie is Beginnend bekend	1	MST-Ziekenhuis
Bekendheid smartapparatuur - Organisatie is Minder bekend	1	St. Jansdal
Bekendheid smartapparatuur - Organisatie weet van bestaan maar geen goed beeld welke in organisatie aanwezig	1	Lindenhout
Bekendheid smartapparatuur - Organisatie redelijk bekend	1	ZGT- Ziekenhuis
Bekendheid smartapparatuur - Organisaties weten van bestaan maar werken er weinig mee i.v.m. organisatorische rompslomp.	1	Mariëlle Stoelinga
Bekendheid smartapparatuur - Protocollencultuur staat het in de weg	1	Mariëlle Stoelinga
Bekendheid smartapparatuur - Iedereen heeft er notie en kennis van	1	Harald Vranken
Soorten smartapparatuur - Smart-tv's	1	MST-Ziekenhuis
Soorten smartapparatuur - Medisch oproepsysteem (Mycom)	1	MST- Ziekenhuis
Soorten smartapparatuur - Slimme wasmachines	1	MST-Ziekenhuis
Soorten smartapparatuur - Slimme sloten	1	MST-Ziekenhuis
Soorten smartapparatuur - Smartwatches voor eigen gebruik	1	MST- Ziekenhuis
Soorten smartapparatuur - Smart plansysteem zaal	1	MST- Ziekenhuis
Soorten smartapparatuur - Slimme thermostaat	1	St. Jansdal
Soorten smartapparatuur - Slimme verlichting	1	St. Jansdal
Soorten smartapparatuur - Smart-tv	1	St. Jansdal
Soorten smartapparatuur - Smart alarm	1	St. Jansdal
Soorten smartapparatuur - Smartwatches voor eigen gebruik	1	St. Jansdal
Soorten smartapparatuur - Smart health zoals pacemakers e.d.	1	St. Jansdal
Soorten smartapparatuur - Smartwatches voor eigen gebruik	1	Lindenhout
Soorten smartapparatuur - Smart-tv	1	Lindenhout
Soorten smartapparatuur - Slimme thermostaat	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme verlichting	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme lampen	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme medische koelkasten met sensors	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme wasmachine	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Smart-tv	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme sloten	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Smart alarm	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Smartwatches voor eigen gebruik	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme meters	1	ZGT-Ziekenhuis
Soorten smartapparatuur - IoT-sensoren	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Smart Health zoals pacemakers e.d.	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme liften	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Slimme deuren	1	ZGT-Ziekenhuis
Soorten smartapparatuur - Alle CT-scans, MRI-scans	1	Mariëlle Stoelinga
Soorten smartapparatuur - Consumermarkt smartapparatuur in toenemende mate	1	Harald Vranken
Gebruik smartapparatuur - Mogelijkheid is er maar zijn nog niet in gebruik	1	MST-Ziekenhuis
Gebruik smartapparatuur - Vooruitgang in businesskant en zorgkant	1	MST-Ziekenhuis
Gebruik smartapparatuur - Smart health meest in gebruik	1	St. Jansdal
Gebruik smartapparatuur - Geen smart health	1	Lindenhout
Gebruik smartapparatuur - Nihil	1	Lindenhout
Gebruik smartapparatuur - Alle smartapparatuur staan in constante verbinding met het intern netwerk	1	ZGT Ziekenhuis
Gebruik smartapparatuur - Zorg buiten de workflow om via eigen apparatuur	1	Mariëlle Stoelinga
Beleid- Inlogcodes intern netwerk	1	MST-Ziekenhuis
Beleid- Overzicht apparaten in verbinding met intern netwerk	1	MST-Ziekenhuis
Beleid- Impact risico wordt bepaald bij aanschaf	1	MST-Ziekenhuis
Beleid- ISO wordt geraadpleegd	1	MST-Ziekenhuis

Beleid- Waarschijnlijk getoetst aan NEN Normen	1	MST-Ziekenhuis
Beleid- Overzicht apparaten in verbinding met intern netwerk	1	St. Jansdal
Beleid- Risicoanalyse bij aanschaf	1	St. Jansdal
Beleid- Checklijsten voor verbinding intern netwerk	1	St. Jansdal
Beleid- Privacy controle nieuwe apparaten	1	St. Jansdal
Beleid- Overzicht apparaten in verbinding met intern netwerk	1	Lindenhout
Beleid- Geen ervaring aanpassen standaardwachtwoorden	1	Lindenhout
Beleid- Noodprocedure aanwezig voor kritische systemen in proces	1	ZGT-Ziekenhuis
Beleid- Risicoanalyse bij aanschaf volgens QMT-aanpak	1	ZGT-Ziekenhuis
Beleid- Overzicht alle aangesloten apparatuur	1	ZGT-Ziekenhuis
Beleid- Patiëntveiligheidscheck bij aanschaf	1	ZGT-Ziekenhuis
Beleid- Security/privacy check bij aanschaf	1	ZGT- Ziekenhuis
Beleid- Bij aanschaf wordt er op diverse Normeringen gelet	1	ZGT- Ziekenhuis
Beleid- Inpassing In ICT-landschap bij aanschaf	1	ZGT- Ziekenhuis
Beleid- Checkprocedure voor aangesloten op intern netwerk	1	ZGT- Ziekenhuis
Beleid- Niet zeker van standaardwachtwoord verandering	1	ZGT- Ziekenhuis
Beleid- Zo snel mogelijk internet laten draaien bij uitval	1	MST-Ziekenhuis
Beleid- Bij uitval internet, verplegers op kamerlamp lopen	1	MST-Ziekenhuis
Beleid- Medewerkers wijzen op cyberrisco's	1	MST-Ziekenhuis
Beleid- Plan voor uitval ICT	1	MST-Ziekenhuis
Beleid- Back-ups patiëntgegevens op ander netwerk	1	MST-Ziekenhuis
Beleid- Normale noodvoorzieningen	1	MST-Ziekenhuis
Beleid- Procedures werken met vertrouwelijke informatie	1	MST-Ziekenhuis
Beleid- Gastnetwerk niet in verbinding vitale systemen	1	MST-Ziekenhuis
Beleid- Stand alone computers	1	MST-Ziekenhuis
Beleid- Medewerkers gewezen op wachtwoordbeleid	1	MST-Ziekenhuis
Beleid- Wie, waar en wanneer patiëntgegevens bekijkt wordt gelogd	1	MST-Ziekenhuis
Beleid- Opschalen bij uitval internet	1	St. Jansdal
Beleid- Business continuity plan aanwezig	1	St. Jansdal
Beleid- IMS moet op niveau blijven en blijvend worden aangepast	1	St. Jansdal
Beleid- Inzicht in apparaten gebruik medewerkers	1	Lindenhout
Beleid- Back-ups patiëntendossiers op aparte lijn	1	Lindenhout
Beleid- Noodprocedure uitval internetsysteem	1	ZGT-Ziekenhuis
Beleid- Kritische processen conform NEN7510/12/13	1	ZGT-Ziekenhuis
Beleid- Bewustwordingstraining handelswijze	1	Deventer Ziekenhuis
Beleid- Kaartensysteem bij overtreding	1	Deventer Ziekenhuis
Beleid- Aanspreekcultuur	1	Deventer Ziekenhuis
Beleid- Beheersplannen niet bedrijfsbreed	1	Deventer Ziekenhuis
Beleid- Back-up voorzieningen	1	Deventer Ziekenhuis
Beleid- Applicatie servicelevels	1	Deventer Ziekenhuis
Beleid- Externe back-up patiëntgegevens	1	Deventer Ziekenhuis
Beleid- Inloggen patiëntsysteem van buitenaf	1	Deventer Ziekenhuis
Beleid- Veiligheid Informatie Managementsysteem	1	Deventer Ziekenhuis
Beleid- Meldsysteem menselijk fouten	1	Deventer Ziekenhuis
Beleid- VMS-thema's kwaliteitssysteem	1	Deventer Ziekenhuis
Beleid- Accu op kritische apparaten	1	Deventer Ziekenhuis
Beleid- Back-up en noodvoorzieningen op voorzieningen	1	Deventer Ziekenhuis
Fysieke beveiliging- Badge systeem	1	MST-Ziekenhuis
Fysieke beveiliging- Hoofdingangen 24 uur per dag open	1	MST-Ziekenhuis
Fysieke beveiliging- Inloggen computer met een pasje	1	MST-Ziekenhuis
Fysieke beveiliging- ICT vrij toegankelijk	1	MST-Ziekenhuis
Code	**Onderzoeksvraag**	**Interview**
Risicobewustheid - TCO en ISO zijn er kenbaar met risico's smartapparatuur	2	MST-Ziekenhuis
Risicobewustheid - Medewerkers zijn laag tot midden bewust van cyberrisico's	2	MST-Ziekenhuis
Risicobewustheid - Medewerkers niet bewust dat ziekenhuis slachtoffer kan worden	2	MST-Ziekenhuis
Risicobewustheid - Kennen de standaard risico's van smartapparatuur	2	St. Jansdal
Risicobewustheid - N.V.T.	2	Lindenhout
Risicobewustheid - Risicoanalyse op smartapparatuur uitgevoerd via QMT-aanpak	2	ZGT-Ziekenhuis

Risicobewustheid - Onvoldoende, hebben het nooit over risico's van smartapparatuur	2	Mariëlle Stoelinga
Risicobewustheid - Medewerkers zoeken de kortste ingang met de minste beveiligingsweerstand	2	Mariëlle Stoelinga
Risicobewustheid - Medewerkers worden geschoold hoe om te gaan met kritische processen	2	Gea Wijn
Risico's smartapparatuur - Berichten op de Mycom zijn beïnvloedbaar	2	MST-Ziekenhuis
Risico's smartapparatuur - Patiëntdata aanpassen	2	Mariëlle Stoelinga
Risico's smartapparatuur - Uitval van systemen	2	Mariëlle Stoelinga
Risico's smartapparatuur - Veel ingangen tot internet	2	Mariëlle Stoelinga
Risico's smartapparatuur – Kritische systemen zijn bereikbaar	2	Mariëlle Stoelinga
Risico's smartapparatuur- Standaard Hecking methodes zijn mogelijk	2	Mariëlle Stoelinga
Risico's smartapparatuur- Medewerker wil zo snel mogelijk bij patiëntdata	2	Mariëlle Stoelinga
Risico's smartapparatuur- Medewerker niet bereid veel wachtwoorden invoeren	2	Mariëlle Stoelinga
Risico's smartapparatuur- Standaardwachtwoorden worden niet veranderd	2	Mariëlle Stoelinga
Risico's smartapparatuur- Nieuw product dus beveiliging nog niet optimaal	2	Mariëlle Stoelinga
Risico's smartapparatuur- Risico's zijn zeldzaam maar groot impact	2	Mariëlle Stoelinga
Risico's smartapparatuur- Gemak is groot, ander wordt eerder getroffen dan ik	2	Mariëlle Stoelinga
Risico's smartapparatuur- Security is niet mee ontworpen	2	Mariëlle Stoelinga
Risico's smartapparatuur- Producten zijn gericht op de consumermarkt	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Zo lek als een mandje	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Kosten	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Time-to-market	2	Marielle Stoelinga
Beveiliging smartapparatuur- beveiliging vereist expertise	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Verkoopdruk	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Te weinig tijd voor beveiliging	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Ligt aan producent	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Geen puckcode zoals bij een mobiele telefoon	2	Mariëlle Stoelinga
Beveiliging smartapparatuur- Soms geen security ingebouwd	2	Harald Vranken
Beveiliging smartapparatuur- Makkelijke standaardwachtwoorden	2	Harald Vranken
Beveiliging smartapparatuur- Wachtwoorden zijn algemeen bekend	2	Harald Vranken
Beveiliging smartapparatuur- Moeilijk om standaard wachtwoord aan te passen	2	Harald Vranken
Beveiliging smartapparatuur- Securitymaatregelen zijn makkelijk te omzeilen	2	Harald Vranken
Beveiliging smartapparatuur- Gericht op consumer market dus minder goed	2	Harald Vranken
Risico's organisaties- Patiëntinformatie niet beschikbaar bij uitval internet	2	MST-Ziekenhuis
Risico's organisaties- Voedselaanbod voor patiënten kan worden beïnvloed	2	MST-Ziekenhuis
Risico's organisaties- Informatie voor zorgverzekeraars kan gehackt worden	2	MST-Ziekenhuis
Risico's organisaties- Meetapparatuur kan verkeerde waarden geven door hack	2	MST-Ziekenhuis
Risico's organisaties- Schade patiënt doordat zorgproces wordt beïnvloed	2	MST-Ziekenhuis
Risico's organisaties- Security wordt omzeild door gemak	2	MST-Ziekenhuis
Risico's organisaties- Nog geen echte incidenten dus geen veiligheidsmaatregel	2	MST-Ziekenhuis
Risico's organisaties- Ziekenhuizen hebben een complexe organisatiestructuur	2	Mariëlle Stoelinga
Risico's organisaties- Minder bereidheid om regels na te leven	2	Mariëlle Stoelinga
Risico's organisaties- Patiëntveiligheid is afhankelijk van patiënten informatie	2	Gea Wijn
Risico's organisaties- Patiëntveiligheid kritische patiënten afhankelijk van vitale functies	2	Gea Wijn
Risico's organisaties- Stroomvoorziening loopt meeste risico	2	Gea Wijn
Beweegredenen crimineel- Verschilt niet veel van niet smartapparatuur	2	Mariëlle Stoelinga
Beweegredenen crimineel- Zorgsector zelfde als andere domeinen	2	Mariëlle Stoelinga
Beweegredenen crimineel- Normale aanvallersprofielen	2	Mariëlle Stoelinga
Code **Onderzoeksvraag**	**Interview**	
Maatregelen informatiebeveiliging- Blijft achter hack aanlopen	3	St. Jansdal
Maatregelen informatiebeveiliging- Bed risicomanagementcyclus af op zorgproces	3	Mariëlle Stoelinga
Maatregelen informatiebeveiliging- Security is basis voor riskmanagement	3	Harald Vranken
Maatregelen informatiebeveiliging- Beleid bepalen	3	Harald Vranken
Maatregelen informatiebeveiliging- Hardware maatregelen	3	Harald Vranken
Maatregelen informatiebeveiliging- Fysieke maatregelen	3	Harald Vranken
Maatregelen informatiebeveiliging- Software updates	3	Harald Vranken
Maatregelen informatiebeveiliging- Procedures voor gebruik	3	Harald Vranken
Maatregelen informatiebeveiliging- Loggen wie waar bijkomt	3	Harald Vranken

Maatregelen informatiebeveiliging- Security incidenten detecteren door logs	3	Harald Vranken
Maatregelen smartapparatuur- Technische maatregelen conform NEN 7510/12/13	3	ZGT-Ziekenhuis
Maatregelen smartapparatuur- Organisatorische maatregelen conform NEN 7510/12/13	3	ZGT-Ziekenhuis
Maatregelen smartapparatuur- Convenant medische hulpmiddelen	3	ZGT-Ziekenhuis
Maatregelen smartapparatuur- QMT Beleid	3	ZGT-Ziekenhuis
Maatregelen smartapparatuur- Meer regels van bovenaf	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Organisatorische maatregelen	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Technische maatregelen	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Psychologische maatregelen	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Maak iemand verantwoordelijk voor security	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Gebruik ISO-standaarden	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Schat risico's in op impact en likelyhood	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Identificeer maatregelen en evalueer continu	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Security awareness training met co-creatie	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Betrek alle stakeholders bij het probleem	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Wachtwoordmanagement	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Acces control	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Algemene maatregelen informatiebeveiliging	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Implementeer de normale informatiebeveiliging	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Goed personeelsbeleid	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Niet aan kritische processen hangen	3	Mariëlle Stoelinga
Maatregelen smartapparatuur- Geen smartapparatuur	3	Mariëlle Stoelinga

Tabel 10 Open codeerschema

B. Axiaal Coderen

Onderzoeksvraag 1

Bekendheid smartapparatuur:

I. Organisaties in zorg

- Beginnend bekend
- Minder bekend
- Weet van bestaan, maar gebruiken het nog niet
- Redelijk bekend
- Iedereen weet ervan

II. Redenen geen gebruik

- Protocollencultuur staat in de weg
- Organisatorische rompslomp

Soorten smartapparatuur in gebruik:

I. Smart Domestic Appliances

- Slimme wasmachines
- Medische koelkasten met sensors

II. Smart Entertainment

- Smart-tv

III. Smart Energy

- Slimme thermostaat

- Slimme meters

IV. Smart Lightning

- Slimme verlichting
- Slimme lampen

V. Smart Motorisation

- IoT-Sensoren
- Slimme liften
- Slimme deuren

VI. Smart Security

- Slimme sloten
- Smart alarm

VII. Smart Communication

- Smartwatches voor eigen gebruik
- Medisch oproepsysteem (Mycom)
- Smart Plansysteem

VIII. Smart Health

- Pacemakers
- Infusiepompen
- CT-Scans
- MRI-Scans
- Overige

Gebruik Smartapparatuur:

I. Ziekenhuizen

- Mogelijkheid is er maar nog niet in gebruik
- Vooruitgang in business kant en zorgkant
- Smart health meeste in gebruik
- Alle smartapparatuur in constante verbinding met intern netwerk

II. Individuele zorginstelling

- Nihil
- Geen Smart Health
- Zorg gaat buiten workflow om via eigen apparatuur

Beleid

I. Smartapparatuur

- Risicoanalyse bij aanschaf
- Er is een overzicht van apparaten die in verbinding staan met het intern netwerk
- ISO wordt geraadpleegd bij aanschaf
- Wordt getoetst aan Normeringen
- Checkprocedure voor verbinding met intern netwerk
- Privacy check bij aanschaf
- Standaardwachtwoorden worden niet aangepast

- Wordt ingepast in ICT-landschap

II. Algemene Informatiebeveiliging

- Noodprocedures bij uitval internetsysteem
- Noodvoorzieningen op back-ups van voorzieningen
- Awareness training cyberrisico's, wachtwoordbeleid en gebruik van apparaten
- Back-up patiëntgegevens op externe systemen
- Gastnetwerk niet in verbinding kritische processen
- Inzicht in gebruik van gegevens en apparaten
- (Veiligheid) Informatiemanagement systeem blijvend bijwerken
- Meldsysteem menselijke fouten
- Accu's op kritische apparaten
- Business Continuity plan aanwezig
- Applicaties hebben servicelevels

Fysieke beveiliging

I. Toegankelijkheid deuren

- Badge systeem
- Hoofdingangen 24 uur per dag open

II. ICT

- Inloggen computer met een pasje
- ICT vrij toegankelijk

Onderzoeksvraag 2

Risicobewustheid

I. Smartapparatuur

- TSCO en ISO zijn er kenbaar mee
- Kennen standaard risico's
- Onvoldoende, hebben het er nooit over

II. Algemene informatiebeveiliging

- Medewerkers zijn laag tot midden bewust van cyberrisico's
- Medewerkers niet bewust van slachtofferschap Ziekenhuis
- Medewerkers zoeken kortste weg met minste beveiligingsweerstand
- Bewust door risicoanalyse uit te voeren via QMT-aanpak

III. Kritische processen

- Medewerkers worden geschoold hoe om te gaan met kritische processen

Beveiliging smartapparatuur

I. Productieproces

- Kosten
- Time-to-market/verkoopdruk
- Te weinig expertise tot beveiliging
- Te weinig tijd voor beveiliging
- Gericht op consumentenmarkt dus beveiliging minder goed

II. Wachtwoorden

- Geen puckcode zoals bij een mobiele telefoon
- Makkelijke standaardwachtwoorden
- Standaardwachtwoorden zijn algemeen bekend
- Moeilijk om wachtwoord aan te passen

III. Technische aspecten

- Zo lek als een mandje
- Soms geen security ingebouwd
- Securitymaatregelen zijn te omzeilen

Risico's Smartapparatuur en organisatie

I. Impact van risico's

- Patiëntengegevens kunnen worden aangepast of niet beschikbaar zijn
- Uitval van systemen
- Kritische systemen zijn bereikbaar
- Risico's zijn zeldzaam maar grote impact
- Voedselaanbod voor patiënt kan worden beïnvloed
- Informatie voor zorgverzekeraars kan gehackt worden
- Meetapparatuur kan verkeerde waarden aangeven
- Patiënt kan schade ondervinden doordat zorgproces wordt beïnvloed
-

II. Technische Risico's

- Veel ingangen tot het internet
- Security is niet mee ontworpen
- Producten zijn gericht op consumentenmarkt
- Nieuw product dus beveiligingsniveau is nog niet hoog
- Berichten op Mycom zijn beïnvloedbaar
- Standaardhackmethodes zijn toepasbaar

III. Gebruikersrisico

- Medewerker wil zo snel mogelijk bij patiëntgegevens
- Medewerker is niet bereid veel wachtwoorden in te voeren
- Standaardwachtwoorden worden niet veranderd
- Gemak, anderen worden eerder getroffen dan ik
- Nog geen echte incidenten dus geen veiligheidsmaatregel
- Medewerkers zijn minder bereid om regels na te leven
- Security wordt omzeild door gemak
- Ziekenhuizen hebben een complexe organisatiestructuur

Beweegredenen crimineel

- Normale aanvallersprofielen
- Zorgsector zelfde als andere domeinen
- Verschilt niet veel van niet-smartapparatuur

Maatregelen

I. Smartapparatuur

- Technische maatregelen conform NEN 7510/12/13
- Organisatorische maatregelen conform NEN 7510/12/13
- Convenant medische hulpmiddelen
- QMT Beleid
- Meer regels van bovenaf
- Psychologische maatregelen
- Schat risico's in op impact en likelyhood
- Identificeer maatregelen en evalueer continu
- Security awareness met co-creatie
- Betrek stakeholders bij het probleem
- Wachtwoordmanagement
- Acces control
- Algemene maatregelen informatiebeveiliging
- Goed personeelsbeleid
- Niet aan kritische processen hangen
- Geen smartapparatuur gebruiken

II. Algemene informatiebeveiliging

- Bed risicomanagementcyclus af op zorgproces
- Security als basis voor risk management
- Procedures hanteren voor gebruik
- Loggen wie waarbij komt en security incidenten detecteren
- Software updates toepassen
- Hardware maatregelen toepassen
- Beleid bepalen
- Implementeer normale informatiebeveiliging

		Respondent 1	Respondent 2	Respondent 3	Respondent 4
Label 1.1	Slimme wasmachines	1	0	0	1
Label 1.2	Slimme koelkasten	1	0	0	0
Label 1.3	Smart-tv	1	1	1	1
Label 1.4	Slimme thermostaat	1	0	1	0
Label 1.5	Slimme meters	1	0	0	0
Label 1.6	Slimme verlichting	1	0	1	0
Label 1.7	Slimme lampen	1	0	0	0
Label 1.8	IoT-sensoren	1	0	0	0
Label 1.9	Slimme liften	1	0	0	0
Label 1.10	Slimme deuren	1	0	0	0
Label 1.11	Slimme sloten	1	0	0	1
Label 1.12	Smart alarm	1	0	0	0
Label 1.13	Smartwatches	1	1	1	1
Label 1.14	Medisch oproepsysteem	0	0	0	1
Label 1.15	Smart plansysteem	0	0	0	1
Label 1.16	Pacemakers	1	0	1	0
Label 1.17	Infusiepompen	1	0	1	0
Label 1.18	Overige smart health	1	0	1	0

Tabel 11 Soorten smartapparatuur per respondent

		Respondent 1	Respondent 2	Respondent 3	Respondent 4
		Ziekenhuis groep Twente	Lindenhout	St Jansdal	Medisch spectrum Twente
Label 1.1	Slimme wasmachines	Wel	Niet	Niet	Wel
Label 1.2	Slimme koelkasten	Wel	Niet	Niet	Niet
Label 1.3	Smart-tv	Wel	Wel	Wel	Wel
Label 1.4	Slimme thermostaat	Wel	Niet	Wel	Niet
Label 1.5	Slimme meters	Wel	Niet	Niet	Niet
Label 1.6	Slimme verlichting	Wel	Niet	Wel	Niet
Label 1.7	Slimme lampen	Wel	Niet	Niet	Niet
Label 1.8	IoT-sensoren	Wel	Niet	Niet	Niet
Label 1.9	Slimme liften	Wel	Niet	Niet	Niet
Label 1.10	Slimme deuren	Wel	Niet	Niet	Niet
Label 1.11	Slimme sloten	Wel	Niet	Niet	Wel
Label 1.12	Smart alarm	Wel	Niet	Niet	Niet
Label 1.13	Smartwatches	Wel	Wel	Wel	Wel
Label 1.14	Medisch oproepsysteem	Niet	Niet	Niet	Wel
Label 1.15	Smart plansysteem	Niet	Niet	Niet	Wel
Label 1.16	Pacemakers	Wel	Niet	Wel	Niet
Label 1.17	Infusiepompen	Wel	Niet	Wel	Niet
Label 1.18	Overige smart health	Wel	Niet	Wel	Niet

Tabel 12 Typen smartapparatuur per organisatie