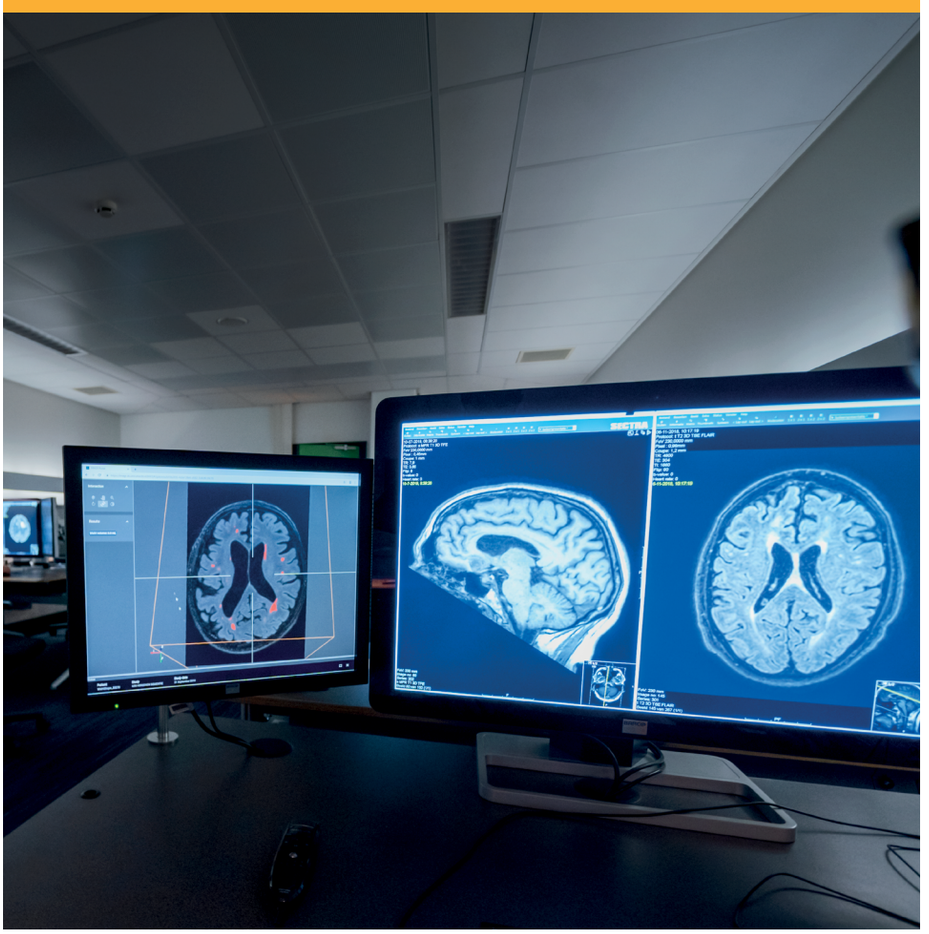
ONDERZOEKSRAAD
VOOR VEILIGHEID

Patiëntveiligheid bij ICT-uitval in ziekenhuizen



Patiëntveiligheid bij ICT-uitval in ziekenhuizen

Den Haag, februari 2020

Coverfoto: Dhr. O. Middendorp

De rapporten van de Onderzoeksraad voor Veiligheid zijn openbaar en te vinden op onderzoeksraad.nl.

De Onderzoeksraad voor Veiligheid

Als zich een ongeval of ramp voordoet, onderzoekt de Onderzoeksraad voor Veiligheid hoe dat heeft kunnen gebeuren, met als doel daar lessen uit te trekken. Op die manier draagt de Onderzoeksraad bij aan het verbeteren van de veiligheid in Nederland. De Raad is onafhankelijk en besluit zelf welke voorvallen hij onderzoekt. Daarbij richt de Raad zich in het bijzonder op situaties waarin mensen voor hun veiligheid afhankelijk zijn van derden, bijvoorbeeld van de overheid of bedrijven. In een aantal gevallen is de Raad verplicht onderzoek te doen. De onderzoeken gaan niet in op schuld of aansprakelijkheid.

Bezoekadres: Lange Voorhout 9
2514 EA Den Haag

Postadres: Postbus 95404
2509 CK Den Haag

Telefoon: 070 333 7000

Website: onderzoeksraad.nl
E-mail: info@onderzoeksraad.nl

INHOUD

BESCHOUWING

De continuïteit van belangrijke maatschappelijke voorzieningen en processen, zoals de drinkwatervoorziening, waterbeheer en de communicatie met en tussen hulpdiensten, is de afgelopen decennia in steeds belangrijkere mate afhankelijk geworden van het ononderbroken functioneren van digitale systemen. Dit geldt ook voor ziekenhuizen, waar ICT is doorgedrongen tot het hart van het zorgproces. Veel handelingen in het ziekenhuis zijn alleen nog mogelijk als de ICT functioneert: het inzien van patiëntgegevens, het maken van afspraken, het doorgeven van laboratoriumuitslagen en het uitgeven van medicijnen. Ziekenhuizen zijn hierdoor inmiddels ook ICT-organisaties geworden. De ICT-afhankelijkheid wordt in de toekomst bovendien alleen maar groter. Zo is de verwachting dat cruciale apparaten rondom het ziekenhuisbed voor hun functioneren steeds meer afhankelijk worden van het ziekenhuisnetwerk en dat monitoring van patiënten op afstand via telefoon of tablet in de toekomst dagelijkse praktijk zal worden. Analoge werkprocessen worden daarbij in gestaag tempo uitgefaseerd, waardoor hier niet meer op teruggevallen kan worden als de ICT uitvalt.

De verregaande digitalisering van de zorg in ziekenhuizen biedt kansen om de zorg te verbeteren. Tegelijkertijd brengt deze ontwikkeling ook nieuwe risico's met zich mee. ICT-uitval is hier een belangrijke van; één defect onderdeel of verkeerde netwerkinstelling kan de primaire zorgprocessen in een ziekenhuis uren- of zelfs dagenlang stilleggen. Dit heeft gevolgen voor de kwaliteit en veiligheid van de zorg voor patiënten. Hoewel er bij de door de Raad onderzochte voorvallen voor zover bekend geen sprake was van letsel bij patiënten, komt wel duidelijk naar voren dat sprake was van een verhoogde kans op schade voor patiënten.

Op basis van het uitgevoerde onderzoek constateert de Raad dat de ziekenhuizen na afloop van de voorvallen de gevolgen voor de patiëntveiligheid hoofdzakelijk afzetten tegen de daadwerkelijk opgetreden schade voor patiënten. De bij de voorvallen opgetreden verhoogde kans op schade bleef grotendeels buiten beschouwing en maakte dikwijls geen deel uit van de evaluaties van de voorvallen. In de evaluaties is bovendien met weinig diepgang gekeken naar de gevolgen van de ICT-uitval voor de veiligheid van de patiënten 'in huis'. Ook de veiligheid van patiënten die vanwege de ICT-storing moesten worden omgeleid, is buiten beeld gebleven. Bovengenoemde punten leiden ertoe dat ziekenhuizen beperkt zicht hebben op de risico's van ICT-uitval voor patiënten. Goed inzicht in de gevolgen van ICT-uitval voor de patiëntveiligheid is een belangrijke voorwaarde voor een adequate beheersing van dit risico.

Dat ICT-uitval een risico is dat serieus genomen moet worden door ziekenhuizen, blijkt ook uit het aantal ICT-storingen dat zich in Nederland heeft voorgedaan de afgelopen jaren. Hoewel er geen centrale registratie plaatsvindt, kan op basis van nieuwsberichten worden afgeleid dat in 2019 tenminste tien ziekenhuisorganisaties werden getroffen door een grootschalige ICT-storing. Dat zijn er fors meer dan vijf jaar geleden, in 2015, toen er in de media over slechts één grootschalige ICT-storing werd gerapporteerd.

Door het veranderend zorglandschap valt door ICT-uitval bovendien steeds vaker de zorgcapaciteit op meerdere plekken in een groter gebied weg. Zo werden bij de tien grootschalige ICT-storingen in 2019 in totaal 28 zorglocaties getroffen.

De ICT-afhankelijkheid in de ziekenhuissector is niet uniek en speelt ook in andere sectoren. Een goed voorbeeld hiervan is de financiële sector, een sector die in Nederland als vitaal wordt aangemerkt.[1] Nederland behoort tot de koplopers van digitaal betalen in Europa. Digitaal betalen is snel en gemakkelijk voor de klant en veilig en efficiënt voor de winkelier. Bij een pinstoring komt echter een groot deel van het betalingsverkeer tot stilstand, omdat veel klanten geen contant geld bij zich hebben of omdat winkeliers alleen nog pinbetalingen accepteren. Daarom hebben banken de afgelopen jaren maatregelen genomen om uitval van het betalingsverkeer (en een daarmee samenhangende maatschappelijke ontwrichting) te voorkomen en wanneer ICT-systemen toch uitvallen, deze zo snel mogelijk weer operationeel te krijgen.

De continuïteit van de zorgverlening is cruciaal voor het welzijn van de Nederlandse bevolking. Het ministerie van VWS heeft een aantal jaar geleden besloten om ziekenhuizen en andere zorgaanbieders niet als vitaal te identificeren. De in 2018 van kracht geworden Wet beveiliging netwerk- en informatiesystemen[2] heeft daarom geen betrekking op ziekenhuizen. Momenteel wordt dit besluit heroverwogen, wat ertoe kan leiden dat ziekenhuizen (al dan niet voor specifieke processen/onderdelen) in 2020 wel zullen moeten voldoen aan de vereisten uit die wet. Het is aan de minister voor Medische Zorg en Sport om te bezien of de bevindingen en conclusies uit dit rapport aanleiding geven om het besluit om ziekenhuizen niet als vitaal aan te merken, te herzien.

De toenemende ICT-afhankelijkheid maakt dat het voor de ziekenhuissector hoe dan ook nodig is om de digitale weerbaarheid op orde te brengen. Dit rapport biedt hiervoor verschillende aanknopingspunten. Het spreekt voor zich dat ziekenhuizen moeten inzetten op het voorkomen van ICT-uitval, bijvoorbeeld door betere inrichting en beheer van het ICT-fundament. Maar dat is niet voldoende. Als gevolg van de complexiteit van ICT-systemen zijn de risico's deels onvoorspelbaar, waardoor uitval niet altijd voorkomen kan worden. Wel kunnen in geval van een ICT-storing de gevolgen zoveel mogelijk worden beperkt. Hiertoe is een goede voorbereiding, ter aanvulling op de veerkracht van het ziekenhuispersoneel, onontbeerlijk. Zo dienen de crisisorganisaties in ziekenhuizen beter toegerust te worden op de specifieke kenmerken van ICT-uitval, zowel met behulp van uitgewerkte planvorming als door training en oefening.

1 Voor de financiële sector zijn bepaalde processen, zoals het betalingsverkeer, aangemerkt als vitaal. Een algehele of gedeeltelijke uitval van deze processen kan zeer grote maatschappelijke en/of financieel-economische gevolgen hebben. Een proces is vitaal als uitval leidt tot:
- meer dan 5 miljard euro schade of 1.0 % daling reëel inkomen.
- meer dan 1.000 doden, ernstig gewonden of chronisch zieken.
- meer dan 100.000 personen ondervinden die emotionele problemen of ernstig maatschappelijke overlevingsproblemen.

2 Wet beveiliging netwerk- en informatiesystemen (Wbni), voorheen ook wel aangeduid als de Cybersecuritywet. De Wbni strekt ter uitvoering van de Europese NIB-richtlijn. Het doel van deze richtlijn is om, ter ondersteuning van het functioneren van onze samenleving en economie, eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen.

Ook dienen afhankelijkheden tussen zorg en ICT in kaart gebracht te worden om te bezien op welke manier ICT-uitval gevolgen kan hebben voor de kwaliteit en veiligheid van de zorg voor patiënten. De systemen die hierbij het meest kritisch blijken, dienen, voor zover redelijkerwijs mogelijk, redundant te worden ingericht. Daarbij is het belangrijk om ICT-systemen periodiek en in samenhang te testen, met als doel ervoor te zorgen dat de kritische zorgprocessen onder alle omstandigheden kunnen blijven functioneren.

Het aantal ICT-storingen in de afgelopen jaren laat zien dat er sprake is van een vraagstuk dat al langer speelt en zich niet tot de drie onderzochte ziekenhuizen beperkt. De Raad acht het van belang dat ziekenhuizen voldoende in beeld hebben hoe afhankelijkheid van ICT kan leiden tot onveilige situaties voor de patiënt. ICT-uitval heeft zich ontwikkeld tot een risico dat, naast meer traditionele risico's (zoals onvoldoende handhygiëne), aandacht verdient van ziekenhuizen. En dan niet alleen op de ICT-afdeling, maar ook binnen de overlegstructuren van medisch personeel en in de bestuurskamer van het ziekenhuis.

AANBEVELINGEN

Ziekenhuizen zijn voor het leveren van goede zorg steeds meer afhankelijk van het goed functioneren van ICT. Uit dit onderzoek blijkt dat ICT-uitval de patiëntveiligheid in het geding kan brengen. De Raad ziet op basis van zijn onderzoek aanknopingspunten om de risico's op ICT-uitval in ziekenhuizen en de gevolgen hiervan voor de patiëntveiligheid vroegtijdig in beeld te krijgen en adequaat te beheersen. Enerzijds door beter te sturen op het voorkomen van uitval van ICT, anderzijds door de organisatie beter voor te bereiden op het beheersen van de gevolgen van uitval van ICT.

De frequentie en duur van ICT-storingen in ziekenhuizen laten zien dat er sprake is van een vraagstuk dat breder speelt. De Raad kiest er daarom voor zich in zijn aanbevelingen niet te beperken tot de drie onderzochte ziekenhuizen, maar zich tot alle ziekenhuizen in Nederland te richten. Om te bevorderen dat ziekenhuizen het vraagstuk gezamenlijk benaderen en van en met elkaar leren om de ICT-risico's beter te beheersen, doet de Onderzoeksraad aanbevelingen aan de twee grootste brancheverenigingen. De Raad ziet ook een rol weggelegd voor de IGJ.

Aan de Nederlandse Vereniging van Ziekenhuizen (NVZ) en de Nederlandse Federatie van Universitair Medische Centra (NFU):

1. Bewerkstellig dat uw leden:

    a. Met het oog op een goede voorbereiding op uitval van ICT, de afhankelijkheden tussen zorg en ICT periodiek in kaart brengen, inclusief de mogelijke risico's voor patiënten die gepaard gaan met ICT-uitval.
    b. Periodiek de ICT-systemen in samenhang testen, om te borgen dat de kritische zorgprocessen onder alle omstandigheden blijven functioneren. Ook dient geoefend te worden met scenario's waarbij de ICT in het ziekenhuis uitvalt. Betrek daar waar zinvol de leveranciers bij deze oefeningen en testen.
    c. Na elke ernstige ICT-uitval evaluaties uitvoeren waarbij ook de (verhoogde kans op) schade voor zowel de patiënten in het ziekenhuis als voor de uitgeweken patiënten diepgaand wordt geanalyseerd. Betrek daarbij waar nodig de partners in de zorgketen.
    d. Over alle drie de hierboven genoemde aspecten jaarlijks publiek verantwoording afleggen.

2. Borg dat ziekenhuizen dit vraagstuk gezamenlijk benaderen en van en met elkaar leren.

Lees verder op de volgende pagina

3. Ontwikkel een praktisch handvat voor ziekenhuizen voor het beheersen van de risico's van uitval van ICT, waarin de in dit rapport genoemde aanknopingspunten worden meegenomen.

4. Ga in regionaal verband na of in geval van ICT-uitval waarbij meerdere ziekenhuislocaties in een regio worden getroffen, de veiligheid van patiënten voldoende is geborgd.

Aan de Inspectie Gezondheidszorg en Jeugd (IGJ):

5. Besteed in het toezicht op ziekenhuizen aandacht aan de punten in bovengenoemde aanbevelingen.

ir. J.R.V.A. Dijsselbloem
Voorzitter van de Onderzoeksraad

mr. C.A.J.F. Verheij
Secretaris-directeur

LIJST VAN AFKORTINGEN

AI	Artificiële Intelligentie
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie
CBT	Crisis Beleidsteam
CIO	*Chief Information Officer*
CMIO	*Chief Medical Information Officer*
CNIO	*Chief Nursing Information Officer*
DAP	Dossier Afspraken en Procedures
EPD	Elektronisch Patiënten Dossier
IC	*Intensive Care*
ICT	Informatie- en Communicatietechnologie
IGJ	Inspectie Gezondheidszorg en Jeugd
ITIL	*Information Technology Infrastructure Library*
JCI	Joint Commission International
MER	*Main Equipment Room*
MOS	Medisch Oproepsysteem
NFU	Nederlandse Federatie van Universitair Medische Centra
NIAZ	Nederlands Instituut voor Accreditatie in de Zorg
NVZ	Nederlandse Vereniging van Ziekenhuizen
OCT	Operationeel Crisisteam
OK	Operatiekamer
SEH	Spoedeisende Hulp
SIT	Spoed Interventie Team
SLA	Service Level Agreement
TIM	Transmuraal Incident Melden
VIM	Veilig Incident Melden
VMS	Veiligheidsmanagementsysteem
VOS	Verpleegkundig Oproepsysteem
VWS	Volksgezondheid, Welzijn en Sport
ZIS	Ziekenhuisinformatiesysteem

LIJST VAN BEGRIPPEN

Artificiële intelligentie (AI)
De intelligentie waarmee machines, software en apparaten zelfstandig problemen oplossen. Zij imiteren hierbij het denkvermogen van de mens.

Controller
Een element in een ICT-systeem dat de functie heeft om data weg te schrijven op, en op te halen van de opslagdisks van de storage.

Crisisplan
Een samenhangend plan waarin een basiswerkwijze staat beschreven voor crisissituaties en waarin een relatie naar onderliggende plannen en procedures is vastgelegd. Hierbij gaat het niet alleen over crisissituaties die de continuïteit van zorg bedreigen, maar over alle soorten crises die een organisatie kunnen raken. Een crisisplan komt niet in de plaats van bestaande plannen (zoals een ziekenhuis rampen opvangplan of continuïteitsplan), maar verbindt deze plannen en zorgt daarmee voor onderlinge samenhang tussen de plannen en procedures. Het biedt een basis om op elke crisis voorbereid te zijn.

Cybersecurity
De beveiliging van ICT tegen aanvallen van buitenaf.

E-health
Het gebruik van informatie- en communicatietechnologie om gezondheid en gezondheidszorg te ondersteunen of te verbeteren, waarbij internettechnologie een belangrijke rol speelt. Zowel de toepassingen voor patiënten, de ondersteuning van het werk van zorgverleners als ook diverse medische apps en systemen vallen hieronder.

ICT-beheer
Het beheren van het ICT-fundament van een organisatie. Het beheer bestaat uit een aantal processen. Daarover wordt onderaan deze lijst van begrippen meer informatie gegeven.

ICT-fundament
Het geheel aan centrale ICT-componenten (hardware en software), die het digitale fundament vormen, waarop alle individuele applicaties en alle medische systemen geïnstalleerd zijn. Hierbij moet men denken aan datacenters, netwerk, servers, dataopslag, databases, (virtuele) werkplekken, communicatiesystemen en beveiligingssystemen.

Informatiebeveiliging
Behoud van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie (zie NEN 7510:1, p.19). Beschikbaarheid is hierbij de eigenschap van het toegankelijk en bruikbaar zijn op verzoek van een bevoegde entiteit (zie NEN 7510-1, p.17). Integriteit is hierbij de eigenschap van nauwkeurigheid en volledigheid (zie NEN 7510-1, p.20).

Vertrouwelijkheid is hierbij de eigenschap dat informatie niet beschikbaar of niet bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen (zie NEN 7510-1, p.26).

Informatie- en Communicatietechnologie
Onder informatietechnologie wordt hardware-, softwareproducten en -diensten verstaan. Tot communicatietechnologie worden communicatieapparatuur en -diensten gerekend. Ook netwerken maken hier onderdeel vanuit.

Main Equipment Room (MER)
Een ruimte waarin centrale ICT-apparatuur is opgesteld.

Medische apparatuur
Elk medisch hulpmiddel dat voor het functioneren afhankelijk is van energie, via het lichtnet of een accu.

Medische technologie
Toepassing van georganiseerde kennis en vaardigheden in de vorm van apparaten, medicijnen, vaccins, procedures en systemen die ontwikkeld zijn om gezondheidsproblemen op te lossen en de kwaliteit van leven te verbeteren.

Medisch personeel
Degenen die direct of indirect bijdragen aan de medische zorg voor patiënten, zoals artsen, verpleegkundigen, laboranten, radiologen etc.

Patiëntveiligheid
Het (nagenoeg) ontbreken van (de kans op) aan de patiënt toegebrachte vermijdbare schade door handelen en/of nalaten van medewerkers of door tekortkomingen in het zorgsysteem.

Schade wordt hierbij gezien als een nadeel voor de patiënt dat door zijn ernst leidt tot verlenging of verzwaring van de behandeling, tijdelijk of blijvend lichamelijk, psychisch en/of sociaal functieverlies, of tot overlijden.

Prospectieve Risico Inventarisatie
Een Prospectieve Risico Inventarisatie is een middel om voor risicovolle processen de risico's gestructureerd inzichtelijk te maken en voor de grootste risico's zoveel mogelijk mitigerende maatregelen te nemen.

Redundant
Meervoudig uitgevoerde voorzieningen en/of systemen.

Root cause analyse
Een systematische aanpak om de oorzaak van een probleem of gebeurtenis op te sporen.

Server
Een computer die in een netwerk een ondersteunende taak vervult.

Service Level Agreement
Een overeenkomst met daarin de afspraken tussen de aanbieder en de afnemer van een dienst of product. In deze overeenkomst ligt vast wat de prestatie-indicatoren en kwaliteitseisen zijn van de te leveren dienst of product, om deze later te kunnen toetsen. Een *Service Level Agreement* kan als afspraak bestaan tussen zowel externe (leverancier) als interne (klant) partijen binnen een organisatie.

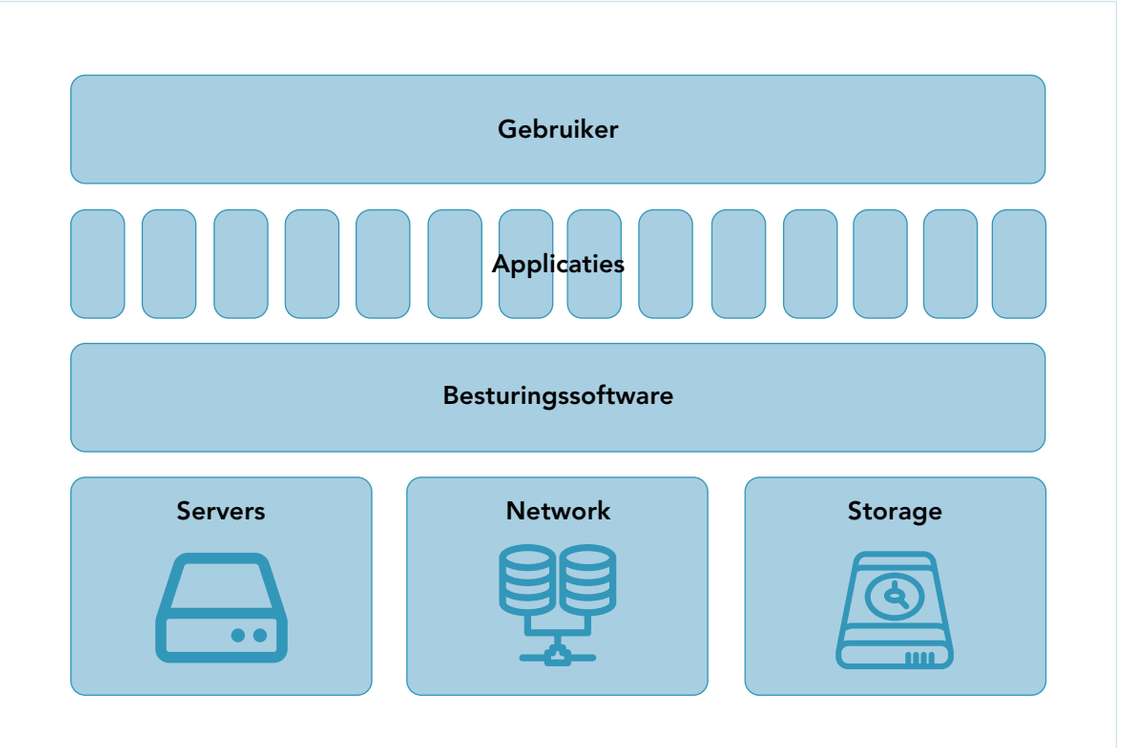
Storage
Systemen die bedoeld zijn om digitale gegevens in op te slaan.

Veilig Incident Melden (VIM)
Bij Veilig Incident Melden worden incidenten en bijna-incidenten in ziekenhuizen gemeld, geanalyseerd en worden verbetermaatregelen voorgesteld. VIM is een methode die ontworpen is om incidenten veilig te melden, te onderzoeken en de oorzaken te categoriseren dichtbij het werkproces.

Virtuele server
Servers worden over het algemeen gevirtualiseerd. Dit wil zeggen dat op dezelfde hardware verschillende servers met verschillende operating systems kunnen draaien. Op dezelfde hardware kan bijvoorbeeld Windows en Linux als operating system worden gebruikt. Voor de gebruiker van zo'n virtuele server is dit niet anders dan een niet-virtuele server. De virtualisatie wordt gedaan door virtualisatiesoftware die tussen de daadwerkelijk hardware en het operating system draait.

Zorgcontinuïteit
Onder zorgcontinuïteit worden de planvorming en de handelingen verstaan die zorginstellingen verrichten ter voorbereiding op, tijdens en na een ramp of crisis om de zorg die zij leveren aan hun patiënten op een verantwoorde wijze te continueren.

Centrale onderdelen ICT-fundament
Digitalisering vereist het opzetten en onderhouden van een ICT-fundament: het geheel aan centrale ICT-componenten (hardware en software), die het digitale fundament vormen, waarop alle individuele applicaties en alle medische systemen geïnstalleerd zijn. Hierbij moet men denken aan datacenters, netwerk, servers, dataopslag, databases, (virtuele) werkplekken, communicatiesystemen en beveiligingssystemen. De centrale onderdelen in ieder ICT-fundament zijn de processing units (Servers), die voor de benodigde rekenkracht zorgen, het netwerk (Network), dat transport van data naar de gewenste plaats mogelijk maakt, en de dataopslag (Storage), die ervoor zorgt dat data vastgelegd, bewaard en digitaal opgehaald kan worden. Op dit ICT-fundament levert de besturingslaag van de hardware (Besturingssoftware) de benodigde functionaliteiten (Applicaties) voor de gebruiker (Gebruiker). Onderstaande figuur geeft een schematische weergave van de opbouw van een ICT-fundament.



Figuur 1: Schematische weergave van de opbouw van een ICT-fundament.

ICT-beheerprocessen

Voor de analyse van het ICT-beheer in ziekenhuizen is gebruik gemaakt van de *Information Technology Infrastructure Library*, oftewel ITIL (v3).[3] ITIL is een reeks van *best practices* en concepten over het inrichten van de beheerprocessen binnen een ICT-organisatie. Het biedt een set richtlijnen, waarbij het de dienstverlening (*services*) als uitgangspunt neemt. De richtlijnen zijn ingedeeld naar de verschillende fases van de *Service Lifecycle*. Per fase zijn processen benoemd voor de voor die fase relevante activiteiten. De onderstaande processen zijn (daar waar relevant) beschouwd in het onderzoek.

Event management

Event management houdt zich bezig met het monitoren van eventuele gebeurtenissen in het systeem (= het *event*). Gebeurtenissen in dit verband kunnen meldingen van een systeem zijn of meldingen van gebruikers. Het doel van het proces is uitsluitend om *events* te monitoren/analyseren en zo nodig tot actie over te gaan.

Incident management

Incident management omvat iedere gebeurtenis die een ICT-dienst verstoort of kan verstoren. Het doel van *incident management* is het zo snel mogelijk herstellen van de ICT-dienstverlening en het minimaliseren van de negatieve impact op de bedrijfsprocessen. Belangrijke elementen bij dit proces zijn: het bepalen van de impact en urgentie van het incident en eventueel benodigde escalatie en het herstel van het incident.

3 In de praktijk bestaan ook andere handvatten voor het inrichten van ICT-beheer. Dat de Onderzoeksraad voor zijn onderzoek gebruik heeft gemaakt van ITIL, wil niet zeggen dat andere kaders niet zouden voldoen.

Capacity management

Capacity management houdt zich bezig met de benodigde capaciteit en performance van ICT-diensten in relatie tot de huidige en toekomstige vereisten van de ICT-gebruikers.

IT service continuity management

IT service continuity management adresseert de continuïteit van bedrijfskritische processen als de onderliggende ICT-dienst uitvalt. *IT service continuity management* richt zich daarmee op de uitzonderlijke situatie dat normale maatregelen gefaald hebben en continuïteit van bedrijfskritische processen geraakt wordt.

Release management

Release management richt zich op het tijdig identificeren, testen en vrijgeven van benodigde soft- en hardware updates in het systeem.

Change management

De waarde van het proces *change management* is vooral de continuïteit van de bedrijfsvoering, ook tijdens het doorvoeren van wijzigingen. Door deze wijzigingen op een gestructureerde manier door te voeren, worden incidenten als gevolg van een change voorkomen.

Service level management

Het doel van *service level management* is om te borgen dat het afgesproken niveau van ICT-dienstverlening wordt bereikt. Dit houdt in dat dit niveau helder wordt gedefinieerd, gedocumenteerd en overeengekomen in de definitiefase. In de operationele fase wordt dit niveau van dienstverlening gemonitord, gemeten, gerapporteerd en geëvalueerd.

Supplier management

Het doel van *supplier management* is om de leveranciers en de diensten die zij bieden te beheren en om naadloze integratie met de eigen ICT-diensten te realiseren, zodat de kwaliteit van de ICT-dienstverlening gewaarborgd is. Bij *supplier management* ligt de aandacht op de relatie tussen de (interne) ICT-dienstverlener en de externe partijen die in deze ICT-dienstverlening een taak of rol vervullen.

1 INLEIDING

1.1 Aanleiding

Op vrijdag 26 januari 2018 vond bij het Radboudumc in Nijmegen een ICT[4]-storing plaats. Medisch personeel[5] ondervond hier hinder van bij het bieden van zorg aan patiënten. Patiëntinformatie was beperkt toegankelijk. Daarnaast was elektronische gegevensuitwisseling niet meer mogelijk, waardoor diverse zorgprocessen minder efficiënt en foutgevoeliger werden. Het laboratorium en de apotheek hadden veel last van de ICT-storing en waren genoodzaakt over te schakelen op noodprocedures. Omdat een veilige behandeling van nieuwe patiënten niet meer gegarandeerd kon worden, kondigde het ziekenhuis in de loop van de middag een algehele opnamestop af.

ICT-uitval in ziekenhuizen

Naast het Radboudumc kregen in 2018 ook andere Nederlandse ziekenhuizen te maken met urenlange ICT-storingen die impact hadden op de zorgverlening. Zo kampte het IJsselland Ziekenhuis in Capelle aan den IJssel op zondag 3 juni met een langdurige ICT-storing. Deze werd gevolgd door een storing in het Dijklander Ziekenhuis[6] in Hoorn op 16 juli en één in het Amsterdam UMC, locatie VUmc[7] in Amsterdam op 23 oktober. Begin 2019 vonden eveneens ICT-storingen plaats in onder meer het Medisch Spectrum Twente en de Noordwest Ziekenhuisgroep. Bij laatstgenoemde storing werden meerdere locaties van de ziekenhuisgroep getroffen, waaronder de locaties in Alkmaar en Den Helder. Hetzelfde geldt voor de ICT-storing in het Tergooi ziekenhuis op 15 augustus 2019, waar de locaties Blaricum en Hilversum getroffen werden, en voor de ICT-storing op 2 september 2019 in Gelre Ziekenhuizen, waar problemen ontstonden bij de locaties Apeldoorn en Zutphen. Later dat jaar volgden er nog ICT-storingen in diverse andere Nederlandse ziekenhuizen. In de meeste gevallen werden daarbij meerdere locaties getroffen. De gevolgen van de ICT-storingen varieerden van het niet toegankelijk zijn van patiëntendossiers en beeldmateriaal tot het uitvallen van alarmsystemen, printers en telefonie, en van het niet kunnen opvragen van digitale beelden, zoals echo's röntgenfoto's en scans, tot het afkondigen van een opnamestop voor de spoedeisende hulp (SEH) en het sluiten van operatiekamers (OK).

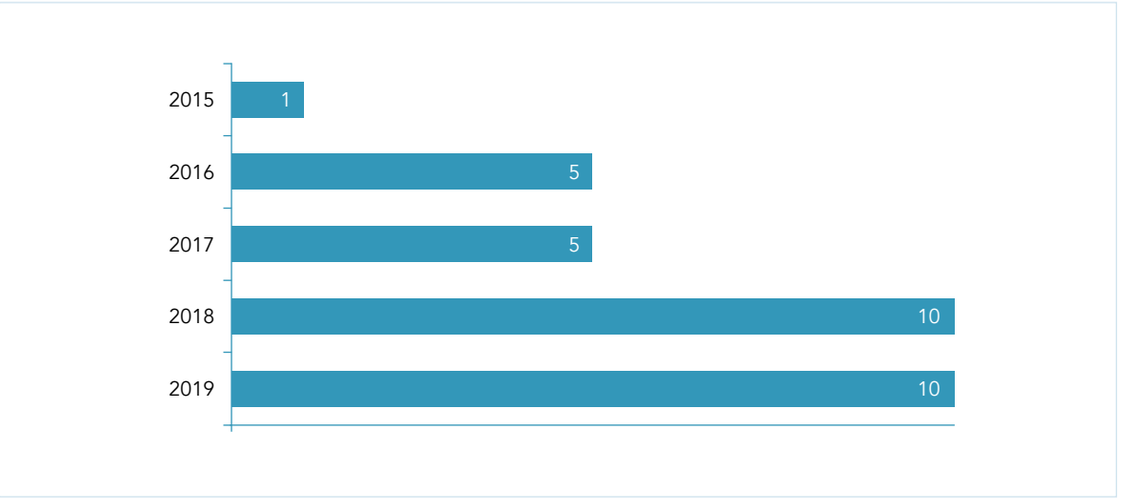
4 Onder informatietechnologie wordt hardware-, softwareproducten en -diensten verstaan. Tot communicatietechnologie worden communicatieapparatuur en -diensten gerekend. Ook netwerken maken hier onderdeel vanuit.

5 Onder medisch personeel wordt verstaan degenen die direct of indirect bijdragen aan de medische zorg voor patiënten, zoals artsen, verpleegkundigen, laboranten, radiologen etc.

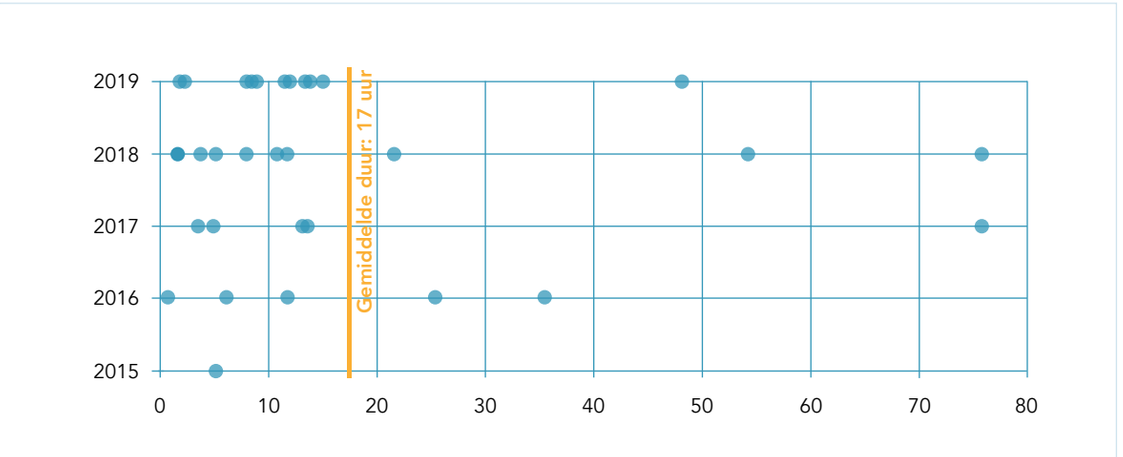
6 Ten tijde van de storing was dit het Westfriesgasthuis in Hoorn. Vanaf januari 2019 zijn het Westfriesgasthuis in Hoorn en het Waterlandziekenhuis in Purmerend gefuseerd en verder gegaan onder de naam Dijklander Ziekenhuis. Daar waar in dit rapport gesproken wordt over het Dijklander Ziekenhuis, wordt bedoeld de locatie Hoorn, voorheen bekend als het Westfriesgasthuis.

7 Op 7 juni 2018 zijn het VUmc en AMC bestuurlijk gefuseerd. Vanaf dat moment zijn de ziekenhuizen verder gegaan als Amsterdam UMC.

In Nederland vindt geen centrale registratie plaats van het aantal en de duur van ICT-storingen in ziekenhuizen. Om die reden heeft de Onderzoeksraad zelf een verkenning uitgevoerd naar het aantal ICT-storingen in ziekenhuizen. Uit deze verkenning blijkt dat bovengenoemde voorbeelden geen uitzonderingen zijn: in de periode 2015-2019 rapporteerden de media 31 keer over grootschalige[8] ICT-storingen in Nederlandse ziekenhuizen (figuur 2).[9] De (gehele of gedeeltelijke) uitval van ICT duurde gemiddeld 17 uur (figuur 3). De storingen vonden plaats in zowel universitair medische centra, als in algemene ziekenhuizen verspreid door het land. In tweederde van de gevallen werden meerdere locaties van één ziekenhuisgroep getroffen (figuur 4).



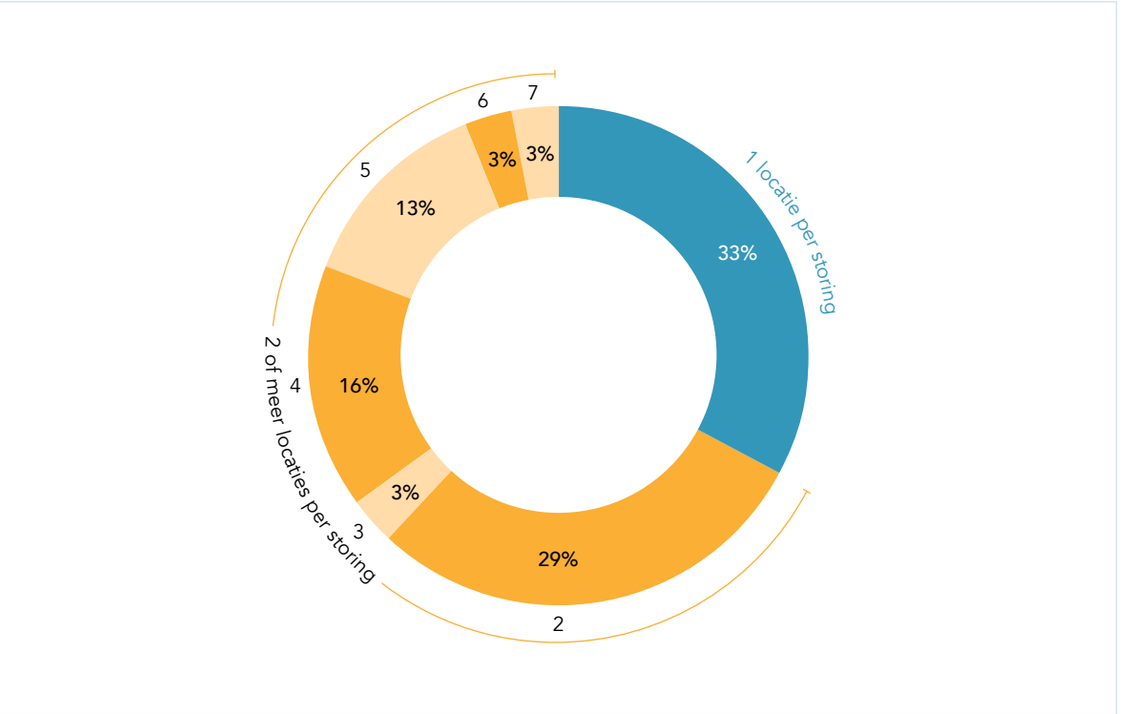
Figuur 2: Aantal ziekenhuizen met ICT-storingen 2015-2019. Ziekenhuisgroepen waarbij meerdere locaties getroffen zijn, zijn in deze figuur geteld als één ICT-storing.



Figuur 3: Duur van ICT-storingen in ziekenhuizen in uren, per jaar.

8 Met grootschalig wordt bedoeld een ICT-storing waarbij de omvang van het incident afdelingsoverstijgend is en in combinatie met de duur van het incident zorgt voor negatieve gevolgen voor de zorgverlening aan patiënten.

9 Om inzicht te krijgen in het aantal keer dat ziekenhuizen grootschalige uitval van ICT hebben ondervonden, wat de duur van deze storingen was en hoeveel locaties daarbij werden getroffen, heeft de Raad landelijke en regionale dagbladen uit de periode 2015-2019 doorzocht en een internetsearch uitgevoerd. De verzamelde informatie is vervolgens geverifieerd bij de betrokken ziekenhuizen. In de tabel zijn uitsluitend storingen opgenomen die ontstaan zijn als gevolg van ICT-gerelateerde factoren. Storingen die optraden als gevolg van stroomstoringen zijn bijvoorbeeld niet in de tabel opgenomen. Daarvan was sprake bij onder meer het Sint Jansdal in Harderwijk (2016 en 2019), het Rijnstate ziekenhuis in Arnhem (2018) en het Canisius Wilhelmina Ziekenhuis in Nijmegen, (2019).



Figuur 4: Aantal getroffen ziekenhuislocaties per storing.

Digitalisering in de zorg

De Onderzoeksraad beziet ICT-uitval in ziekenhuizen tegen de achtergrond van de digitalisering[10] van de zorg. Digitalisering heeft geleid tot grote veranderingen in de samenleving. Digitale technologie wordt steeds complexer door de toename van rekenkracht, dataficatie en connectiviteit[11]:

- *Rekenkracht:* De rekenkracht van computers is toegenomen waardoor het mogelijk is om steeds meer (complexe) processen te automatiseren. Algoritmen maken het bovendien mogelijk om grotere hoeveelheden data te verwerken, sneller beslissingen te kunnen nemen en deze beslissingen deels in handen van systemen te leggen. Wanneer deze processen verstoord worden, kan dat tot gevolg hebben dat ze onveilig worden of uitvallen.
- *Dataficatie:* Steeds meer maatschappelijke processen zijn gebaseerd op informatiestromen. De hoeveelheid data groeit en de toepassing ervan is toegenomen, en daarmee ook de afhankelijkheid ervan. Data worden bovendien ingezet voor tal van processen die de mens niet of nauwelijks meer zelf kan uitvoeren en krijgt een bepalender positie. Wanneer data niet beschikbaar zijn, leidt dit vanwege de koppeling aan processen tot problemen.

10 Digitaliseren betekent letterlijk '[informatie, red] omzetten in digitale vorm ([in, red] nullen en enen)' (Van Dale). In de context van dit rapport gebruikt de Raad deze term om de ontwikkeling weer te geven van het gebruik van analoge toepassingen naar het toenemende gebruik van digitale technologie.

11 Onderstaande informatie is grotendeels ontleend aan het rapport 'Voorbereiden op digitale ontwrichting, Wetenschappelijke Raad voor het Regeringsbeleid, 2019.

- *Connectiviteit:* Dataverzameling- en verwerking en computergestuurde besluitvorming zijn geen los van elkaar verlopende processen, maar onderling verbonden in netwerken. Het aantal internetgebruikers, het aantal aan het internet verbonden apparaten en de hoeveelheid data die uitgewisseld wordt, neemt nog steeds toe. Het gebruik van *cloudcomputing* en de opkomst van het *Internet of Things* (IoT) en artificiële intelligentie zullen de connectiviteit naar verwachting verder versterken. Goed functionerende netwerken zijn belangrijk voor de continuïteit van maatschappelijke processen.

Digitalisering is ook doorgedrongen tot de zorgsector, waaronder in ziekenhuizen.[12] Dit biedt enerzijds kansen om de kwaliteit en efficiëntie van zorg te verbeteren. Anderzijds maakt het ziekenhuizen in toenemende mate afhankelijk van ICT (en het goed functioneren daarvan) voor het leveren van goede zorg. De Onderzoeksraad vraagt zich gegeven deze ontwikkelingen af in hoeverre de uitval van ICT de veiligheid van patiënten in gevaar kan brengen. Daarom heeft de Raad een onderzoek ingesteld naar de ICT-storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis, in relatie tot de patiëntveiligheid. Deze incidenten zijn geselecteerd naar type en grootte van het ziekenhuis, het moment waarop de storing zich heeft voorgedaan (kort voor of tijdens het lopende onderzoek), de duur en omvang van de storing.

1.2 Doelstelling

De Onderzoeksraad wil met dit rapport een bijdrage leveren aan de (verdere) verbetering van de patiëntveiligheid in Nederlandse ziekenhuizen. Hij doet dat door lessen te trekken uit bovengenoemde drie ICT-storingen om ziekenhuizen in Nederland beter in staat te stellen om i) ICT-storingen te voorkomen en te bestrijden; en ii) de veiligheidsrisico's voor patiënten als gevolg van ICT-storingen te kunnen beheersen. Het is nadrukkelijk niet het doel van het onderzoek om een oordeel te vellen over de drie onderzochte ziekenhuizen noch om lessen te formuleren die alleen op hen betrekking hebben. De drie incidenten zijn benut als cases om zicht te krijgen op het algemene vraagstuk van patiëntveiligheid in relatie tot ICT-uitval. De Raad streeft ernaar de lessen te trekken op een dusdanig niveau, dat deze van nut zijn voor alle ziekenhuizen.

1.3 Onderzoeksvragen

De volgende hoofdvraag staat centraal in dit onderzoek:

> Hoe kunnen ziekenhuizen de risico's van ICT-storingen voor de patiëntveiligheid op adequate wijze beheersen?

12 Zie hoofdstuk 2 voor meer informatie over digitalisering van de ziekenhuiszorg.

De hoofdvraag valt uiteen in de volgende deelvragen:

1. Hoe zijn de ICT-storingen ontstaan, bestreden en de gevolgen ervan beheerst?
2. Welke risico's brengen ICT-storingen met zich mee voor patiëntveiligheid?
3. Hoe worden de risico's van ICT-storingen voor patiëntveiligheid binnen de onderzochte ziekenhuizen beheerst?
4. Welke organisatiefactoren binnen de onderzochte ziekenhuizen belemmeren een adequate beheersing van de risico's van ICT-uitval voor de patiëntveiligheid?
5. Hoe kan het systeem voor een adequate beheersing van de risico's van ICT-uitval voor de patiëntveiligheid worden verbeterd?

1.4 Onderzoeksaanpak

Om de onderzoeksvragen te beantwoorden heeft de Onderzoeksraad onderzoek gedaan naar ICT-storingen bij drie ziekenhuizen. Daarbij zijn verschillende methoden voor gegevensverzameling en -analyse gebruikt. Voor het in kaart brengen van de digitalisering van de (ziekenhuis)zorg is voornamelijk literatuur bestudeerd en zijn gesprekken met experts gevoerd. De directe oorzaken van de storingen, de (potentiële) effecten van de storingen op de patiëntveiligheid, de incidentbestrijding en de crisisbeheersing zijn onderzocht door het verzamelen en analyseren van gegevens uit interviews en documenten zoals verslagen van de crisisoverleggen, evaluatieverslagen en logbestanden (met behulp van een analysetool Splunk). Om de achterliggende factoren van de ICT-storingen en crisisbeheersing te kunnen blootleggen, is middels interviews en documentenstudie op hoofdlijnen gekeken naar beheer en inrichting van het ICT-fundament en naar de (voorbereiding van de) crisisbeheersing in de onderzochte ziekenhuizen. Om inzicht te krijgen in aanknopingspunten voor adequate beheersing van risico's van ICT-storingen, heeft de Onderzoeksraad tevens aan de hand van interviews en documentstudie onderzocht welke factoren binnen de organisatie kunnen verklaren hoe de operationele onvolkomenheden konden optreden. Duiding en analyse vonden voor een belangrijk deel plaats in teamsessies door de verzamelde gegevens af te zetten tegen het referentiekader zoals beschreven in paragraaf 1.6.

Naast uitgebreid onderzoek naar de storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis heeft de Raad drie andere storingen die zich gedurende de looptijd van het onderzoek voordeden, op hoofdlijnen beschouwd. Het gaat om storingen in het Amsterdam UMC (locatie VUmc), de Noordwest Ziekenhuisgroep en het Medisch Spectrum Twente. Deze incidenten zijn in het rapport opgenomen om te laten zien dat de drie door de Onderzoeksraad onderzochte incidenten niet op zichzelf staan. Voor de beschouwing van deze voorvallen zijn documenten opgevraagd bij deze ziekenhuizen, zoals crisisplannen[13], verslagen van de crisisoverleggen, evaluatieverslagen

13 Een crisisplan is een samenhangend plan waarin een basiswerkwijze staat beschreven voor crisissituaties en waarin een relatie naar onderliggende plannen en procedures is vastgelegd. Hierbij gaat het niet alleen over crisissituaties die de continuïteit van zorg bedreigen, maar over alle soorten crises die een organisatie kunnen raken. Een crisisplan komt niet in de plaats van bestaande plannen (zoals een ziekenhuis rampen opvangplan of continuïteitsplan), maar verbindt deze plannen en zorgt daarmee voor onderlinge samenhang tussen de plannen en procedures. Het biedt een basis om op elke crisis voorbereid te zijn.

en *root cause analyses*[14]. Deze documenten zijn bestudeerd en waar nodig heeft de Onderzoeksraad aanvullende vragen gesteld om de bevindingen van de ziekenhuizen beter te kunnen duiden. Een beschrijving van de oorzaak van deze storingen, de incidentbestrijding en het functioneren van de crisisorganisatie staat in bijlage F.[15] In een enkel geval wordt in voorliggend rapport naar deze voorvallen verwezen.

Bijlage A bevat een gedetailleerde onderzoeksverantwoording.

1.5 Afbakening

Dit onderzoek richt zich op ziekenhuisorganisaties, omdat zij verantwoordelijk zijn voor de kwaliteit van zorg. Zorginstellingen kunnen echter niet los worden gezien van het systeem waar zij onderdeel van uitmaken. Daarom komt soms ook de rol van andere partijen ter sprake, zoals het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) en de Inspectie voor Gezondheidszorg en Jeugd (IGJ).

Bij het begrip informatiebeveiliging wordt doorgaans onderscheid gemaakt tussen beschikbaarheid, integriteit en vertrouwelijkheid.[16] Dit onderzoek beperkt zich tot de beschikbaarheid. Daarmee vallen onderwerpen als datalekken en het vertrouwelijk omgaan met informatie buiten de scope van het onderzoek. Hoewel integriteit van data geen onderdeel uitmaakt van dit onderzoek, hebben maatregelen die hierop genomen worden wel invloed op de patiëntveiligheid. Dit is bijvoorbeeld aan de orde wanneer ziekenhuizen na een ICT-storing patiëntendossiers moeten actualiseren en controleren. De integriteit van data komt daarom zijdelings aan bod in dit onderzoek.

Waar in dit onderzoek wordt gesproken over ziekenhuizen, gaat het over de instellingen voor medisch specialistische zorg, die zowel klinische als poliklinische zorg verlenen. Dit betreft de algemene ziekenhuizen[17], de universitair medische centra en de categorale instellingen.

ICT-uitval kan veroorzaakt worden door intentioneel handelen en niet-intentioneel handelen. De voor dit onderzoek geselecteerde voorvallen kenmerken zich door onbedoelde (niet-intentionele) uitval van ICT-systemen in ziekenhuizen, waardoor maatregelen genomen moesten worden om schade aan patiënten te voorkomen. De gekozen afbakening van dit onderzoek hangt enerzijds samen met het feit dat er ten tijde van de start van het onderzoek in Nederland, voor zover bekend bij de Onderzoeksraad, geen voorval had plaatsgevonden waarbij een cyberaanval had geleid

14 Een root cause analyse is een systematische aanpak om de oorzaak van een probleem of gebeurtenis op te sporen.
15 Bijlage F is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.
16 Deze drie begrippen vormen samen de BIV. Beschikbaarheid is hierbij de eigenschap van het toegankelijk en bruikbaar zijn op verzoek van een bevoegde entiteit (zie NEN 7510-1, p.17). Integriteit is hierbij de eigenschap van nauwkeurigheid en volledigheid (zie NEN 7510-1, p.20). Vertrouwelijkheid is hierbij de eigenschap dat informatie niet beschikbaar of niet bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen (zie NEN 7510-1, p.26).
17 Inclusief de deelverzameling topklinische ziekenhuizen.

tot ICT-uitval in een ziekenhuis.[18] Anderzijds hangt de keuze voor de afbakening samen met het beeld dat er nog weinig aandacht is voor risico's van ICT-uitval voor de patiëntveiligheid als gevolg van niet-intentioneel handelen.[19] De Raad denkt vanuit de gekozen invalshoek een toegevoegde waarde te kunnen bieden voor digitale veiligheid in ziekenhuizen in het algemeen, en het beheersen van risico's van ICT-uitval in ziekenhuizen voor de patiëntveiligheid in het bijzonder.

1.6 Referentiekader

De Onderzoeksraad hanteert bij zijn onderzoeken een referentiekader waarin de belangrijkste uitgangpunten voor de veiligheid betreffende het onderzoeksthema beschreven zijn. Het referentiekader vormt daarmee tevens een belangrijke basis voor de aanbevelingen. Deze paragraaf beschrijft de uitgangspunten die de Raad in dit onderzoek hanteert.

1.6.1 Patiëntveiligheid

Zorginstellingen zijn verantwoordelijk voor de kwaliteit van zorg. Goede zorg is zorg van goede kwaliteit en goed niveau[20], waarbij de patiënt onder andere juiste, tijdige en veilige zorg ontvangt. Als het gaat om veiligheid van zorg worden de begrippen 'patiëntveiligheid' en 'veilige zorg' in de medische literatuur en de media door elkaar gebruikt.[21, 22] Omdat de term patiëntveiligheid beter aansluit bij het taalgebruik van de onderzochte ziekenhuizen, kiest de Onderzoeksraad in zijn analyse voor de term patiëntveiligheid.

18 In het buitenland hadden ten tijde van de start van het onderzoek wel cyberaanvallen op ziekenhuizen plaatsgevonden. In 2017 werden in Groot-Brittannië bijvoorbeeld meerdere ziekenhuizen het slachtoffer van een ransomware aanval (de WannaCry ransomware aanval). Kort voor publicatie van dit onderzoek vond een cyberaanval plaats op een Nederlands ziekenhuis. Op 15 januari 2020 hebben hackers namelijk een poging gedaan in te breken in de digitale systemen van het Medisch Centrum Leeuwarden. Het ziekenhuis besloot daarop alle dataverkeer met de buitenwereld tijdelijk af te sluiten.

19 De Onderzoeksraad komt mede op basis van literatuurstudie en bestudering van brieven, die het ministerie van VWS in recente jaren aan de Tweede Kamer heeft gestuurd, tot de constatering dat er meer aandacht is voor security, en privacy-gerelateerde vraagstukken dan voor safety-gerelateerde vraagstukken als het gaat om ICT in de zorg.

20 De Wet kwaliteit, klachten en geschillen zorg stelt in artikel 2, lid a, dat goede zorg, zorg van goede kwaliteit en goed niveau is "die in ieder geval veilig, doeltreffend, doelmatig en cliëntgericht is, tijdig wordt verleend, en is afgestemd op de reële behoefte van de cliënt".

21 Signalering Ethiek en Gezondheid, Centrum voor Ethiek en Gezondheid, *Veilige zorg, goede zorg*?, p.14.

22 Wel kiezen instellingen in hun communicatie meestal voor één van de twee termen. Zo kiest de NEN-8009 2019,: 2018 voor de term patiëntveiligheid, het Centrum voor Ethiek en Gezondheid voor de term veilige zorg, en lijkt de Rijksoverheid in officiële stukken een voorkeur te hebben voor de term patiëntveiligheid, terwijl in de publiekscommunicatie ook de term veilige zorg wordt gebruikt.

De Onderzoeksraad verstaat onder patiëntveiligheid[23]:

"Het (nagenoeg) ontbreken van (de kans op) aan de patiënt toegebrachte vermijdbare schade door handelen en/of nalaten van medewerkers of door tekortkomingen in het zorgsysteem."

Schade wordt hierbij gezien als een "nadeel voor de patiënt dat door zijn ernst leidt tot verlenging of verzwaring van de behandeling, tijdelijk of blijvend lichamelijk, psychisch en/of sociaal functieverlies, of tot overlijden."

In bovenstaande definitie vormt zowel het (nagenoeg) ontbreken van vermijdbare schade als het (nagenoeg) ontbreken van de *kans op* vermijdbare schade onderdeel van patiëntveiligheid. De (kans op) schade kan daarbij uit verschillende vormen van ernstig nadeel bestaan. Waar in dit rapport gesproken wordt over een verhoogde kans op schade, bedoelt de Onderzoeksraad de verhoogde kans op vermijdbare schade ten opzichte van de situatie waarin er geen sprake geweest zou zijn van ICT-uitval. Doet zich een verhoogde kans op schade voor, dan beschouwt de Onderzoeksraad dat als een aantasting van de patiëntveiligheid.

1.6.2 Kwaliteit van zorg

De Onderzoeksraad hanteert als uitgangspunt voor dit onderzoek dat patiënten erop moeten kunnen vertrouwen dat de zorg die zij in ziekenhuizen ontvangen, van goede kwaliteit en veilig is. Daarvoor is het nodig dat het ICT-fundament stabiel is, informatie continu beschikbaar is en gedeeld kan worden, en dat aan het ICT-netwerk verbonden apparatuur moet kunnen functioneren.

Digitalisering is belangrijk om zorg - waaronder de patiëntveiligheid - te verbeteren. Tegelijkertijd kan digitalisering ook leiden tot nieuwe veiligheidsrisico's. Ziekenhuizen dienen oog te hebben voor deze risico's en adequate maatregelen te nemen om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid, adequaat te beheersen.

1.6.3 Verantwoordelijkheid voor het beheersen van risico's

De Onderzoekraad hanteert als uitgangspunt dat de betrokken partijen de verantwoordelijkheid hebben om de veiligheidsrisico's in een systeem zo systematisch en goed mogelijk te beheersen. Ziekenhuizen dienen te beschikken over een veiligheidsmanagementsysteem zoals aangegeven in de NEN 8009: 2018.[24] Daarnaast

23 Het betreft hier de definitie van patiëntveiligheid en van schade zoals geformuleerd in NEN 8009:2018 'Veiligheidsmanagementsysteem voor ziekenhuizen en instellingen die ziekenhuiszorg verlenen', p.9.

24 NEN 8009: 2018. '*Veiligheidsmanagementsysteem voor ziekenhuizen en instellingen die ziekenhuiszorg verlenen*'. Deze norm richt zich op het beheersen van risico's voor de patiëntveiligheid en op het benutten van kansen om vermijdbare schade aan patiënten te voorkomen. Ziekenhuizen moeten vanaf eind 2023 een gecertificeerd of geaccrediteerd veiligheidsmanagementsysteem hebben ingevoerd conform de eisen van NEN 8009. De opdrachtgevende partijen voor de NEN-norm zijn de Nederlandse Vereniging van Ziekenhuizen, de Nederlandse Federatie voor Universitair Medische Centra, Federatie Medisch Specialisten en Verpleegkundigen & Verzorgenden Nederland. Zij hebben zich gecommitteerd aan de geformuleerde basiseisen in de NEN 8009.

dienen zij aan diverse normen te voldoen op het terrein van informatiebeveiliging, zoals de NEN-7510 (2017) en NEN-7512 (2015)[25] en het Convenant "*Veilige Toepassing van Medische Technologie in de medisch specialistische zorg*" (Convenant Medische Technologie)[26]. De IGJ houdt toezicht op *e-health*[27] op basis van het Toetsingskader "*Inzet van e-health door zorgaanbieders*".[28] Dit moet bijdragen aan veilige zorg en aan het terugdringen van vermijdbare schade van patiënten door aandacht te besteden aan veiligheidsrisico's. ICT-risico's voor patiëntveiligheid maken hier onderdeel vanuit.

1.6.4 Borging van zorgcontinuïteit

De Onderzoeksraad verwacht dat ziekenhuizen de risico's op ICT-uitval trachten te beheersen, door zowel maatregelen te treffen om ICT-storingen te voorkomen als maatregelen te treffen om, bij optreden van een ICT-storing, zorgcontinuïteit te waarborgen.

Bij het voorkomen van ICT-storingen is de inrichting en het beheer van het ICT-fundament van belang. Een hoogwaardig niveau van de inrichting en het beheer van het ICT-fundament draagt echter niet alleen bij aan het voorkomen van storingen, maar is ook belangrijk om storingen sneller te verhelpen als deze zich onverhoopt toch voordoen. De Onderzoeksraad acht het daarom van belang dat ziekenhuizen voor de kritische elementen van hun ICT-fundament redundante[29] systemen inrichten. Daarnaast vindt de Onderzoeksraad het belangrijk dat ICT-systemen *realtime* en continu gemonitord worden. Potentiële problemen in het functioneren van de ICT-systemen kunnen daardoor tijdig in beeld komen waardoor de kans op ICT-uitval verkleint. Tot slot vindt de Onderzoeksraad het op orde brengen en houden van beheerprocessen van belang, waaronder het opstellen van procedures voor zowel het uitvoeren van werkzaamheden aan het ICT-fundament als voor de directe bestrijding van ICT-uitval.

Ziekenhuizen worden – door de toenemende verwevenheid van ICT-systemen en hiermee gepaard gaande hogere kwaliteitseisen – steeds afhankelijker van externe partijen, zoals fabrikanten, leveranciers en beheer- en onderhoudspartijen. Het ICT-beheer binnen ziekenhuizen vindt daarom in toenemende mate plaats vanuit een samenwerking met andere partijen en/of wordt aan andere partijen uitbesteed.

25 NEN 7510:2017. Deze norm richt zich op het handhaven van de beschikbaarheid, integriteit en vertrouwelijkheid van patiëntinformatie. Ziekenhuizen zijn verplicht (interne) audits uit te (laten) voeren m.b.t. de informatiebeveiliging (NEN 7510-1: 35). NEN 7512 gaat in op de uitwisseling van gegevens en beschrijft eisen en maatregelen die nodig zijn en is gericht op afspraken die communicerende partijen hierover zullen moeten maken. De IGJ toetst als externe partij aan de hand van NEN-normen of zorginstellingen de juiste maatregelen treffen voor invoering en handhaving van informatiebeveiliging.

26 Het Convenant Medische Technologie (2018) is een praktische uitwerking en concretisering van een aantal minimumveiligheidseisen zoals deze zijn verankerd in de NTA 8009:2011, nu NEN 8009:2018.

27 E-health staat voor het gebruik van informatie- en communicatietechnologie om gezondheid en gezondheidszorg te ondersteunen of te verbeteren, waarbij internettechnologie een belangrijke rol speelt. Zowel de toepassingen voor patiënten, de ondersteuning van het werk van zorgverleners als ook diverse medische apps en systemen vallen hieronder.

28 Toetsingskader IGJ "*Inzet van e-health door zorgaanbieders*", gebaseerd op Wkkgz, NEN 8009, NEN 8028, het Convenant Medische Technologie (2018) en het Kwaliteitskader verpleeghuiszorg.

29 Redundant betekent dat een systeem of voorziening meervoudig is uitgevoerd.

De Onderzoeksraad acht het van belang dat ziekenhuizen overzicht houden over het totale ICT-fundament, over voldoende expertise beschikken om hun regierol adequaat in te kunnen vullen, en heldere afspraken maken over de verdeling van de taken en verantwoordelijkheden tussen de ICT-afdeling van het ziekenhuis en externe partijen.

De complexiteit van het ICT-fundament en de mate van onderlinge verbondenheid van de verschillende systemen in het ziekenhuis, maken het waarschijnlijk dat ICT-incidenten zich op een zeker moment zullen voordoen; uitval van ICT kan niet altijd worden voorkomen.[30] Daarom moeten ziekenhuizen, gegeven hun verantwoordelijkheid voor de kwaliteit van zorg, zich inspannen om de zorgcontinuïteit voor, tijdens en na een incident te waarborgen. Daarvoor is het onder meer nodig dat ziekenhuizen een crisisplan inclusief ICT-scenario hebben, een bijpassende crisisorganisatie inrichten, en hun personeel opleiden, trainen en oefenen in het beheersen van de gevolgen van ICT-uitval voor de patiëntveiligheid. Ook is het van belang dat systemen getest worden, om te borgen dat kritische zorgprocessen onder alle omstandigheden gecontinueerd kunnen worden.[31]

Ongeacht de mate van beschikbaarheid die door de totale keten van applicaties en het ICT-fundament kan worden gegarandeerd, dienen ziekenhuizen ervoor te zorgen dat de kritische informatie voor klinische patiënten 100% beschikbaar is. Dat betekent dan ook dat alle kritische klinische processen erop voorbereid moeten zijn dat op elk moment de door de ICT-geleverde informatie beschikbaar moet blijven. Dat kan voor een deel worden opgevangen door noodvoorzieningen (offline tablets, die continu worden gevoed met de actuele kritische data bijvoorbeeld). Tevens moeten er voorzieningen zijn om registratie van verrichtingen te doen gedurende de periode dat ICT uit de lucht is, en een plan om de integriteit van data ook na een storing te kunnen garanderen.

1.6.5 Leren van incidenten

Het evalueren van incidenten, en daaropvolgend treffen van verbetermaatregelen, draagt bij aan een adequate beheersing van risico's van ICT-uitval voor patiëntveiligheid. Het analyseren van ICT-storingen is van belang om inzicht te krijgen in de directe en achterliggende oorzaken van het incident, opdat zowel op technisch als op beheerniveau de juiste verbetermaatregelen kunnen worden getroffen.

30 Ongeacht de oorzaak van de uitval, zoals verstoringen, storingen, stroomuitval etc.
31 NEN 7510-2: 2017, 17.1 en 17.2.

1.7 Leeswijzer

Dit rapport is als volgt opgebouwd:

- Hoofdstuk 2 biedt achtergrondinformatie over digitalisering van de zorg en beschrijft de manier waarop dit ertoe heeft geleid dat ziekenhuizen voor het verlenen van zorg afhankelijk zijn geworden van ICT.
- Hoofdstuk 3 geeft antwoord op de vraag welke factoren een rol hebben gespeeld bij het ontstaan van de onderzochte ICT-storingen, bij de bestrijding ervan en bij de beheersing van de gevolgen.
- Hoofdstuk 4 laat zien welke risico's voor de patiëntveiligheid zich kunnen voordoen bij ICT-uitval.
- Hoofdstuk 5 gaat in op de aanknopingspunten om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid goed in beeld te krijgen en te beheersen.
- Hoofdstuk 6 bevat de hoofdconclusies van dit onderzoek.
- Hoofdstuk 7 bevat de aanbevelingen naar aanleiding van dit onderzoek.

2 ICT-AFHANKELIJKHEID ZORG

Dit hoofdstuk geeft een schets van de digitalisering van de zorg in Nederlandse ziekenhuizen. Deze digitalisering vormt namelijk de achtergrond waartegen de Raad de voorvallen, en de impact daarvan op de patiëntveiligheid, heeft onderzocht. Dit hoofdstuk start in paragraaf 2.1 met een korte uiteenzetting over de digitaliseringstrend in ziekenhuizen in verleden, heden en toekomst. Vervolgens wordt in paragraaf 2.2. beschreven dat de digitalisering van invloed is op elk proces in het ziekenhuis. Dat dit ervoor heeft gezorgd dat ziekenhuizen voor hun functioneren afhankelijk zijn geworden van ICT is het onderwerp van paragraaf 2.3, waarna in paragraaf 2.4 zal worden toegelicht dat dit een kwetsbare afhankelijkheid betreft. In paragraaf 2.5 wordt dit hoofdstuk kort samengevat.

2.1 Digitale revolutie in de zorg

Sinds de intrede van de computer in de jaren zestig heeft zich een digitale revolutie voltrokken in de (medisch-specialistische) zorg. Met name de afgelopen tien à twintig jaar zijn de (zorg)processen in ziekenhuizen verregaand gedigitaliseerd. Dit heeft niet alleen de bedrijfsvoering van ziekenhuizen efficiënter gemaakt, maar ook de kwaliteit en veiligheid van de zorg verbeterd. Diagnoses kunnen in een eerder stadium en met grotere nauwkeurigheid worden gesteld en behandelmethoden zijn verbeterd. De digitalisering van de gegevensverwerking heeft er verder voor gezorgd dat informatie op meer uniforme wijze ingevoerd wordt, op meerdere plekken beschikbaar is en door meerdere zorgverleners tegelijk geraadpleegd kan worden.[32] Het zorgt er bovendien voor dat patiëntendossiers niet meer kwijtraken en onleesbare doktershandschriften tot de verleden tijd behoren. De digitalisering heeft tevens als groot voordeel dat patiënten direct inzage kunnen hebben in hun medisch dossier, en zodoende een actieve rol kunnen spelen in hun eigen behandelingsproces.

Wetenschappelijk onderzoek laat zien dat het diagnosticeren van borstkanker significant verbetert als de diagnose van de patholoog en de bevindingen van de radioloog, gecombineerd worden met voorspellingen van de computer. Hierdoor daalde de foutmarge in het bepalen van de grootte en de locatie van tumoren met 85 procent.[33]

32 Hierbij dient opgemerkt te worden dat veel zorgverleners in de praktijk ervaren dat het delen van informatie nog vele belemmeringen kent.

33 Dit voorbeeld is overgenomen uit het rapport *Ziekenhuiszorg in cijfers 2018* van de Nederlandse Vereniging van Ziekenhuizen (NVZ).

Deze voordelen van digitalisering zorgen ervoor dat ook nu nog op dagelijkse basis nieuwe digitale toepassingen in ziekenhuizen worden geïntroduceerd. De toename van technische mogelijkheden, bijvoorbeeld door ontwikkelingen op het gebied van artificiële intelligentie (AI)[34] en *virtual reality*, zal er bovendien voor zorgen dat dit zich in de (nabije) toekomst zal voortzetten. Ook andere ontwikkelingen in de (ziekenhuis)sector zullen daaraan bijdragen. Denk hierbij aan de noodzaak om de uitgaven aan medisch-specialistische zorg te beheersen[35], het daarmee samenhangende streven van ziekenhuizen om zorg dichterbij de patiënt te organiseren en de toenemende afhankelijkheid van andere partijen – zoals huisartsen en apothekers – om goede zorg te kunnen leveren.

2.2 Digitalisering van (zorg)processen

De kern van de digitalisering van de zorg wordt gevormd door de digitalisering van gegevensverwerking, oftewel het aanmaken, bewerken, opslaan en delen van (patiënt) informatie. Het elektronisch patiëntendossier (EPD) speelt bij deze gedigitaliseerde gegevensverwerking een centrale rol. Alle ziekenhuizen in Nederland hebben inmiddels een volwassen EPD. Daarmee zitten ze (minimaal) op schaal 3 van het *Electronic Medical Record Adoption Model* (EMRAM)[36], een model waarmee de mate waarin de informatieverwerking in ziekenhuizen is gedigitaliseerd, kan worden gemeten. In dit model worden zeven niveaus onderscheiden. Een ziekenhuis op niveau 1 maakt geen gebruik van digitale informatiesystemen en bij niveau 7 is sprake van een papierloos ziekenhuis. Op dit moment hebben twee ziekenhuizen in Nederland niveau 7 bereikt (Radboudumc en Ziekenhuis St. Jansdal) en zitten twee ziekenhuizen op niveau 6 (het Onze Lieve Vrouwe Gasthuis en het Medisch Centrum Leeuwarden).[37, 38]

De digitalisering van de zorg betreft niet alleen de gegevensverwerking in het EPD, maar ook de diagnose en behandeling van patiënten. Ook alle medisch diagnostische processen zijn in hoge mate gedigitaliseerd, vooral omdat daarbij gebruik gemaakt wordt van gedigitaliseerde gegevensstromen en –verwerking. Daarnaast worden ook steeds meer digitale technologieën ontwikkeld en geïmplementeerd voor het analyseren van meetgegevens (bijvoorbeeld laboratoriumwaarden) en beeldmateriaal (bijvoorbeeld radiologie, echo's). AI speelt in toenemende mate een belangrijke rol in het ondersteunen van de medisch specialist bij het vaststellen van een diagnose en het opstellen van een prognose, medicatieplan of een behandelvoorstel.

34 Artificiële intelligentie is de intelligentie waarmee machines, software en apparaten zelfstandig problemen oplossen. Zij imiteren hierbij het denkvermogen van de mens.
35 Afspraken hierover zijn vastgelegd in het *Bestuurlijk akkoord medisch-specialistische zorg 2019 t/m 2022*, 4 juni 2018.
36 https://www.himss.eu/healthcare-providers/emram.
37 https://www.himssanalytics.org/europe/stage-6-7-achievement.
38 Overigens hebben niet alle Nederlandse ziekenhuizen een assessment laten doen. Er zijn waarschijnlijk meer ziekenhuizen die op niveau 6 of 7 geclassificeerd kunnen worden.

In het Radboudumc wordt vanaf medio 2019 AI ingezet om onderzoekers te ondersteunen bij het ontdekken van kankercellen. Hierbij wordt gebruik gemaakt van een computer die met behulp van AI weefsel tot op detailniveau kan fotograferen en analyseren. Via een robotarm worden glaasjes met weefsel gefotografeerd waarna duizenden foto's worden samengevoegd tot één beeld dat vervolgens door de patholoog wordt bekeken. Met deze (digitale) techniek kunnen naar verwachting snellere en betere diagnoses worden gesteld.[39]

Ook het (toenemend) gebruik van operatierobots is een voorbeeld van digitalisering van zorgprocessen, omdat ook dit vaak computergestuurde, datagedreven en in het ziekenhuisnetwerk verbonden apparaten zijn. Een betrekkelijk nieuwe ontwikkeling is 3D-printing, waarbij op basis van digitaal beeldmateriaal op maat gemaakte protheses of operatiehulpstukken geprint worden. Daarnaast wordt meer en meer gebruik gemaakt van mobiele apps en wearables om de toestand van patiënten op afstand te monitoren. Het contact met patiënten vindt al lang niet altijd meer plaats op de poliklinieken in de ziekenhuizen, maar ook digitaal via een patiëntportaal en video-consult.

Zowel het IJsselland Ziekenhuis als het Dijklander Ziekenhuis zijn in de tweede helft van 2019 gestart met het op afstand monitoren van een groep patiënten met chronisch hartfalen. De patiënten meten thuis zelf regelmatig hun bloeddruk, hartslag en gewicht. Deze waarden worden via een app doorgegeven aan de zorgverleners in het ziekenhuis. Als de patiënt afwijkende waarden laat zien, wordt de verpleegkundige daar direct op geattendeerd door de software en kan er actie worden ondernomen.[40]

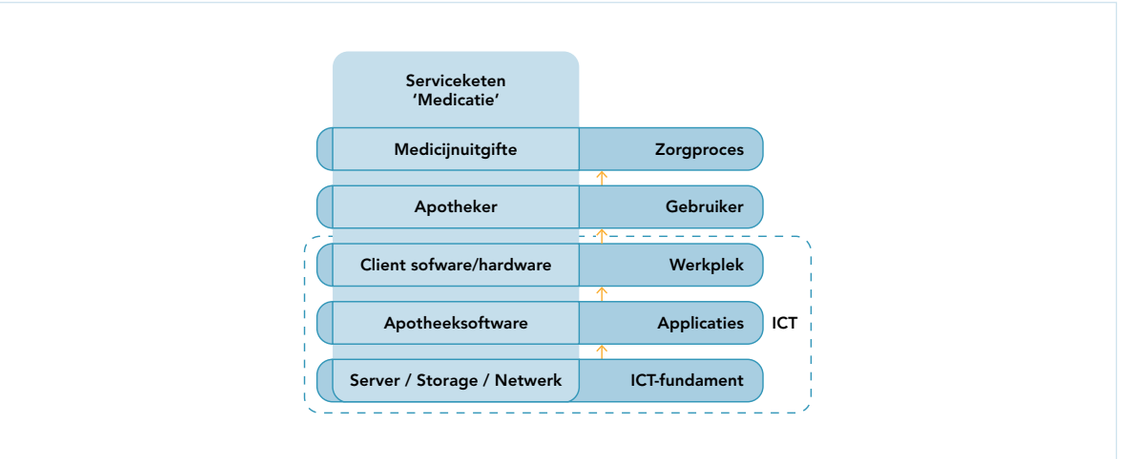
Naast de gegevenswerking en de zorgprocessen zijn ook andere processen in het ziekenhuis gedigitaliseerd. Daarbij kan gedacht worden aan bedrijfsvoeringsprocessen, zoals de administratie, en zorgondersteunende processen, zoals gebouwbeheer, logistiek en inkoop- en voorradenbeheer. Bovendien zijn in vrijwel alle ziekenhuizen ook de communicatiemiddelen, zoals de telefonie en de alarmeringssystemen aan het bed (bijvoorbeeld het Verpleegkundig Oproepsysteem (VOS)), gedigitaliseerd.

39 Voorbeeld gebaseerd op: ICT&Health, *Radboudumc gaat kankercellen via AI analyseren*. 15 oktober 2019, https://www.icthealth.nl/nieuws/radboudumc-gaat-kankercellen-via-ai-analyseren/.

40 Voorbeeld gebaseerd op nieuwsberichten van het IJsselland Ziekenhuis (*IJsselland Ziekenhuis start met monitoring hartfalenpatiënten op afstand*, 8 oktober 2019) en het Dijklander Ziekenhuis (*Hartfalen in de gaten houden met een app*, 24 september 2019)

2.3 Afhankelijkheid van ICT

De digitalisering van ziekenhuiszorg heeft ervoor gezorgd dat ziekenhuizen voor het leveren van goede en veilige zorg in zeer hoge mate afhankelijk zijn geworden van ICT. Dit belang van ICT voor het goed verlopen van de gedigitaliseerde (zorg)processen in ziekenhuizen kan worden geschetst aan de hand van de (vereenvoudigde weergave van de) serviceketen[41] van de medicatievoorziening in een ziekenhuis (figuur 5).



Figuur 5: Schematische weergave van serviceketen medicatie in een ziekenhuis.

Om medicijnen te kunnen uitgeven (het zorgproces), dient de ziekenhuisapotheker (de gebruiker) toegang te hebben tot de gegevens (informatie) van een patiënt. Om toegang te krijgen tot die informatie, logt de gebruiker in op zijn werkplek (de cliëntsoft-/hardware). Na inloggen heeft de gebruiker toegang tot de gewenste informatie via een applicatie (de apotheeksoftware). Om deze informatie op te slaan en toegankelijk te maken heeft de applicatie een ICT-fundament nodig: een (of meer) server(s)[42] om de applicatie te laten functioneren, een database en storage[43] om gegevens op te slaan en een netwerk om applicatieservers, databases, storageservers en gebruikers met elkaar te verbinden. Alle ICT-elementen in deze keten dienen goed te functioneren om de gebruiker (de ziekenhuisapotheker) het zorgproces (medicijnuitgifte) uit te kunnen laten voeren.

In een gemiddeld ziekenhuis zijn tientallen van deze serviceketens te identificeren. Voor al deze ketens geldt dat de (zorg)processen in die ketens afhankelijk zijn van het functioneren van ICT. Uitval van ICT zorgt ervoor dat het (reguliere) proces wordt verstoord, waardoor het leveren van veilige en goede zorg in het geding kan komen. Het zijn niet alleen verstoringen in de systemen die direct in de serviceketen betrokken zijn die van invloed kunnen zijn op de processen in de serviceketen. Ook verstoringen in systemen in aanpalende ketens kunnen invloed hebben op de zorgprocessen. Denk hierbij aan het agendasysteem van poliklinieken, dat door een ICT-storing niet toegankelijk is, waardoor geen afspraken voor patiënten en/of personeel geraadpleegd

41 Een serviceketen geeft een overzicht van alle ICT-componenten die voor een specifiek proces aanwezig moeten zijn.
42 Een server is een computer die in een netwerk een ondersteunende taak vervult.
43 De storage bestaat uit de systemen die bedoeld zijn om digitale gegevens in op te slaan.

en/of gemaakt kunnen worden. Een dergelijke storing heeft een grote invloed op een groot aantal zorgprocessen in meerdere serviceketens. Een ander voorbeeld is een storing in het telefonieplatform. Telefonische bereikbaarheid en communicatie is een essentieel element in vrijwel alle zorggerelateerde serviceketens. Een grote storing in het telefonieplatform heeft direct grote impact op vrijwel alle zorgprocessen.

Bij deze afhankelijkheid van ICT is het van belang dat de invloed van ICT, en dan met name van het ICT-fundament, vaak de individuele (zorg)processen overstijgt. De implementatie van (bijvoorbeeld) een nieuwe dataopslagmodule zal, indien dit misgaat en leidt tot uitval van het gehele data-opslagplatform, van invloed zijn op de meeste serviceketens. Daarmee worden alle (zorg)processen die deel uitmaken van deze ketens tegelijkertijd geraakt. Het goed functioneren van met name de centrale voorzieningen van het ICT-fundament is van essentieel belang voor het goed functioneren van alle (zorg)processen in een ziekenhuis; een klein probleem kan leiden tot een grote verstoring van (zorg)processen in het ziekenhuis (of in meerdere ziekenhuizen als die van dezelfde centrale voorzieningen gebruik maken).

De werking van medische apparatuur[44] is steeds meer afhankelijk van de beschikbaarheid van het ICT-fundament. Waar het momenteel nog zo wordt ingericht dat alle apparatuur, die in kritische situaties gebruikt wordt, bij een storing in het ICT-fundament terug kan vallen naar een stand alone modus, is het de vraag in hoeverre dit in de toekomst, bij verdergaande digitalisering, nog het geval zal zijn. In stand alone modus is bovendien geen gegevensverwerking (verslaglegging) en integratie naar de zorgsystemen (EPD) meer mogelijk, waardoor de apparatuur nog slechts beperkt van nut is. Denk hierbij bijvoorbeeld aan een MRI-scanner die wel een scan kan maken, maar geen beelden kan doorgeven.[45] Het onderzoek kan op zichzelf regulier plaatsvinden, maar het analyseproces van het beeldmateriaal en de daaropvolgende vaststelling van de diagnose door de behandelend arts wordt bemoeilijkt.

Storingen in individuele applicaties hebben doorgaans een kleinere impact op het zorgproces dan storingen in het ICT-fundament. Als bijvoorbeeld het ERP-systeem[46] uitvalt, kunnen vrijwel alle zorgprocessen probleemloos doorlopen, omdat de zorgapplicaties hier slechts op indirecte wijze mee verbonden zijn. Een uitzondering hierop is het EPD. Als het EPD niet beschikbaar is (bijvoorbeeld bij een upgrade of bij een technische storing), dan zijn alle zorgprocessen die het EPD gebruiken (en dat zijn de meeste) betrokken.

44 Voor het begrip medische apparatuur zijn verschillende afbakeningen en definities beschikbaar. In dit rapport wordt aangesloten bij de definitie van Ecorys (*Sectorstudie medische hulpmiddelen Onderzoek naar de structuur en werking van de markt voor medische hulpmiddelen*, 2011): "Elk medisch hulpmiddel dat voor het functioneren afhankelijk is van energie, via het lichtnet of een accu."

45 De MRI-scanners die op dit moment gebruikt worden, slaan de beelden dan wel op, zodat ze later alsnog doorgegeven zouden kunnen worden.

46 Een ERP-systeem (ERP staat voor Enterprise Resource Planning) is een softwarepakket dat logistieke, administratieve en financiële bedrijfsprocessen automatiseert.

2.4 Kwetsbare afhankelijkheid

Het ICT-landschap in ziekenhuizen is de afgelopen decennia in kleine stapjes geëvolueerd tot een complex geheel. Een gemiddeld ziekenhuis heeft honderden applicaties en systemen draaien. Deze zijn op verschillende momenten in de tijd geïmplementeerd en op evolutionaire wijze in gebruik genomen. Deze systemen en applicaties interacteren op diverse manieren met elkaar en zijn (functioneel gezien) nauw met elkaar verbonden. Oftewel, ze zijn voor het functioneren in belangrijke mate afhankelijk van elkaar.

Het functioneren van ICT-systemen in ziekenhuizen is daarnaast ook steeds meer afhankelijk van externe partijen. Dit wordt veroorzaakt doordat onderdelen van het ICT-fundament worden uitbesteed aan ICT-leveranciers (outsourcing) en/of gedeeld met andere (ziekenhuis)organisaties (shared services). Ook is er een tendens waar te nemen dat steeds meer applicaties als Software as a service (SaaS)[47] aangeboden worden, waarbij de informatie steeds meer verspreid wordt over datacenters buiten het ziekenhuis en zelfs buiten de landsgrenzen. De afhankelijkheden van derden maken de keten van afhankelijkheden en de daarmee samenhangende complexiteit groter.

Het gevolg van deze complexiteit en afhankelijkheden is dat een relatief eenvoudige ICT-storing onvoorspelbare, verstrekkende en razendsnelle gevolgen kan hebben voor de rest van het systeemlandschap. Het is vaak moeilijk om snel de oorzaak te achterhalen en ook de aard en impact van de storing is niet altijd meteen duidelijk. De reacties tussen de verschillende onderdelen van het ICT-fundament zijn in zekere mate onvoorspelbaar en daarmee moeilijk te beheersen. Dit maakt het risico op ICT-uitval en de gevolgen daarvan voor de patiënten moeilijk te overzien en te beheersen. De ICT-storing op 15 januari 2019 bij de Noordwest Ziekenhuisgroep illustreert deze problematiek.

De Noordwest Ziekenhuisgroep heeft de opslag van haar data uitbesteed aan een externe provider. Voor de opslag van de data wordt door de externe provider een storageserver gebruikt. Deze storageserver wordt door meer klanten gebruikt zonder dat deze klanten bij elkaars data kunnen komen. De Noordwest Ziekenhuizengroep heeft op deze storageserver (net als de andere klanten) zijn eigen Storage Virtual Machine (SVM). Een kopieer-actie van de externe provider op een van hun eigen servers (dus niet van Noordwest Ziekenhuisgroep) leidde tot een ICT-storing waardoor uiteindelijk het EPD in het ziekenhuis niet meer beschikbaar was. Zie bijlage F voor een uitgebreide beschrijving van dit voorval.[48]

47 Software as a service. Hierbij worden applicaties door externe partijen gehost (in een *cloud*) en voor klanten beschikbaar gemaakt via het internet.
48 Bijlage F is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

2.5 Samenvattend

De (medisch-specialistische) zorg is de afgelopen decennia in hoog tempo gedigitaliseerd. Dit gaat verder dan alleen elektronische gegevensverwerking via een EPD. Alle primaire zorgprocessen zijn in belangrijke mate afhankelijk van ICT. Dat geldt ook voor de zorgondersteunende processen die van invloed zijn op de patiëntenzorg. Dit heeft ervoor gezorgd dat ziekenhuizen voor het leveren van veilige en goede zorg in zeer hoge mate afhankelijk zijn van het goed functioneren van ICT.

Door de complexiteit van het ICT-landschap en de afhankelijkheden daarbinnen en daarbuiten (eventueel met derde partijen), kan een ICT-storing snel leiden tot grootschalige uitval van ICT. Het gevolg daarvan is dat een belangrijk deel van de (zorg) processen in het ziekenhuis wordt geraakt. In hoofdstuk 4 wordt belicht op welke manieren dit van invloed kan zijn op de patiëntveiligheid. In hoofdstuk 3 wordt eerst ingegaan op de oorzaak van de storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis. Ook belicht dat hoofdstuk de wijze waarop de incidenten zijn bestreden en het verloop van de crisisbeheersing.

3 ANALYSE VAN VOORVALLEN

In dit hoofdstuk wordt ingegaan op de voorvallen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis. De Raad heeft daarbij gekeken naar de directe en achterliggende oorzaken van de ICT-uitval, de incidentbestrijding en de crisisbeheersing.[49]

Paragraaf 3.1 geeft een beschrijving van de voorvallen op hoofdlijnen, geordend aan de hand van de drie onderdelen: oorzaak ICT-uitval, incidentbestrijding en crisisbeheersing. In paragraaf 3.2 worden de voorvaloverstijgende factoren beschreven, waarvan de Raad heeft geconstateerd dat ze een belangrijke rol hebben gespeeld bij de voorvallen in twee of meer van de onderzochte ziekenhuizen. In paragraaf 3.3 staat de conclusie van dit hoofdstuk.

3.1 Beschrijving voorvallen

3.1.1 Radboudumc

Op 26 januari 2018 ontving de Servicedesk ICT van het Radboudumc rond 10:30 uur meldingen van medewerkers van het ziekenhuis dat er problemen waren met de ICT-voorzieningen. Netwerkschijven waren niet bereikbaar en verschillende programma's, zoals het laboratoriuminformatiesysteem, werkten niet meer. Al snel bleek de uitval van een storageserver het probleem, waarna de ICT-afdeling de fabrikant van de storage inschakelde om op zoek te gaan naar de oorzaak van de uitval. Rond 16:00 uur zag het ziekenhuis zich genoodzaakt een algehele opnamestop af te kondigen (vanaf 16:30 uur). Rond 18:00 uur was de storage weer hersteld en kon worden begonnen met het opstarten van systemen en applicaties. Rond 21:00 uur was 95% van de systemen weer operationeel en om 21:30 uur werd de opnamestop opgeheven. Hiermee duurde de ICT-storing ongeveer elf uur.

Oorzaak ICT-uitval

Op 26 januari 2018 voerde een ICT-medewerker omstreeks 10:00 uur werkzaamheden uit op de applicatieservers van het Radboudumc. De werkzaamheden activeerden een softwarefout, die leidde tot de uitval van één van de controllers van de storage. De functie van een controller is het wegschrijven en ophalen van data op de opslagdisks. De werkzaamheden creëerden vanwege een softwarefout onbedoeld een inconsistentie in de database met metadata voor de storage, waardoor deze corrupt raakte. Dit leidde tot het afsluiten van de toegang van de controller tot de disks. Aangezien de controllers elkaar bij falen overnemen, liepen alle controllers hier uiteindelijk achter elkaar tegenaan,

49 Een uitgebreide weergave van de resultaten van het onderzoek per voorval is terug te vinden in bijlage D (*technische onderzoeksrapportages*) en bijlage E (*crisisbeheersing*). Deze bijlagen staan op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

waardoor er geen toegang tot de gehele storage meer mogelijk was. Daardoor viel de storageserver rond 10:30 uur uit. Geografische spreiding van de datareplicatie op het storagesysteem had deze uitval kunnen voorkomen. Vanwege de migratie van het oude naar het nieuwe systeem was besloten om deze geografische datareplicatie nog niet toe te passen, maar dit te combineren met de upgrade van de nieuwere versie van een van de applicaties (het laboratoriuminformatiesysteem GLIMS). Het uitvallen van de storageserver leidde daardoor direct tot uitval van een deel van de ICT-voorzieningen op de werkvloer.

Incidentbestrijding
ICT-medewerkers van het Radboudumc merkten rond 10:15 uur voor het eerst op dat er iets misging met de controllers in het storagesysteem. Ze zagen dat meerdere controllers uitvielen, maar begrepen niet goed wat de oorzaak hiervan was, ook omdat een relatie tussen de werkzaamheden op de applicatieserver en uitval van het storagesysteem niet voor de hand liggend was. Twee minuten nadat de laatste controller van het systeem uitviel, maakte de ICT-afdeling van het Radboudumc een melding van de storing aan bij de fabrikant van het storagesysteem. Het incident werd daarbij door de medewerkers van het ziekenhuis en de fabrikant aangeduid als hoogste prioriteit (prioriteit 1). De ICT-medewerkers van het ziekenhuis moesten vervolgens wachten totdat de fabrikant het probleem in beeld had en tot een oplossing was gekomen.

De fabrikant schatte de situatie direct als ernstig in en mobiliseerde alle aanwezige kennis om de storing te analyseren. Kort na de initiële melding vroeg de fabrikant het ziekenhuis om *snapshots* van het systeem te maken en deze op te sturen voor verdere analyse. Een uur na de start van de storing waren de logfiles verzameld en werden ze vanuit het ziekenhuis naar de fabrikant gestuurd voor de analyse. De fabrikant stuurde de logfiles vervolgens door naar specialisten voor verdere analyse. Die achterhaalden de oorzaak van de storing. Op dat moment werd duidelijk dat sprake was van een softwarefout. Om 17:15 uur was een *work around* beschikbaar, waarna de systemen weer opgestart konden worden. Dit nam nog een paar uur in beslag, waarna rond 21:00 uur 95% van de systemen weer operationeel was.

Het kostte de fabrikant vervolgens ongeveer twee maanden om de precieze oorzaak van het probleem te vinden. Op 5 april 2018 kwam de fabrikant met een *softwarepatch*. Daarmee werd de fout in de software verholpen en kon het ziekenhuis het storagesysteem weer normaal (zonder de *work around*) gebruiken.

Crisisbeheersing
Ongeveer een half uur na het uitvallen van de storageserver werd de crisisorganisatie van het Radboudumc geactiveerd. De impact van de storing op de zorg leek in de eerste uren nog beperkt te zijn. De acute zorgafdelingen (zoals de Intensive Care (IC) en de SEH) hadden er op dat moment namelijk beperkt last van. Alle apparatuur werkte nog en ook de patiëntinformatie was digitaal beschikbaar (via het EPD).[50] Deze afdelingen waren dan ook niet overgegaan op noodprocedures. Een aantal andere afdelingen (zoals het

50 Het EPD van het ziekenhuis draaide op een andere storageserver.

laboratorium en de apotheek) daarentegen hadden veel last van de ICT-uitval en waren wel overgegaan op noodprocedures.

In de loop van de middag werd het voor de crisisorganisatie steeds duidelijker dat de ICT-uitval impact had op de zorg. Zo werd het voor de artsen in het ziekenhuis steeds minder goed mogelijk om snel en accuraat diagnoses te stellen, doordat de daarbij ondersteunende afdelingen steeds slechter functioneerden. Zo was het voor het laboratorium steeds moeilijker om spoedbepalingen tijdig uit te voeren en de resultaten tijdig naar de arts te communiceren, omdat ze waren overgeschakeld op handmatig werken. Uitslagen van onderzoeken konden hierdoor bijvoorbeeld niet meer digitaal gecommuniceerd worden en dus moest men deze doorbellen.

Op het moment dat de crisisorganisatie daarbovenop het bericht ontving van de ICT-afdeling dat het nog uren zou kunnen duren voordat de ICT-storing opgelost zou zijn, werd besloten om vanaf 16:30 uur een volledige opnamestop af te kondigen. De crisisfunctionarissen en het dienstdoende lid van de raad van bestuur vonden namelijk dat een veilige behandeling van nieuwe patiënten niet meer gegarandeerd kon worden. Doordat er geen nieuwe patiënten meer opgenomen zouden worden, kon de beschikbare capaciteit op de afdelingen volledig aangewend worden voor de al opgenomen patiënten.

Toen rond 21:00 uur duidelijk werd dat 95% van de systemen weer werkte, besloot het ziekenhuis de volledige opnamestop vanaf 21:30 uur op te heffen, de crisisorganisatie af te schalen en over te gaan naar reguliere aansturing van de organisatie.

3.1.2 IJsselland Ziekenhuis

Op 3 juni 2018 viel rond 01:30 uur het netwerk van het IJsselland Ziekenhuis kortstondig uit. Dit had tot gevolg dat een groot aantal (virtuele) servers[51] werd uitgeschakeld.[52] Door een misverstand tussen het ziekenhuis en de externe netwerkbeheerder werd het herstarten van de servers enkele uren vertraagd. Ook het herstarten zelf nam een aantal uur in beslag, waardoor sprake was van een langdurige storing. Omdat de verantwoorde zorg voor nieuwe patiënten in het geding kwam, kondigde het ziekenhuis vanaf 07:00 uur een algehele opnamestop af. Eén patient werd verplaatst naar een ander ziekenhuis. Ook werd een aantal patiënten verplaatst naar andere afdelingen en/of intensiever gemonitord. Nadat de ICT-systemen vanaf 13:30 uur weer werkten, werd de opnamestop opgeheven. De ICT-storing heeft hiermee in totaal ongeveer 12 uur geduurd.

51 Servers worden over het algemeen gevirtualiseerd. Dit wil zeggen dat op dezelfde hardware verschillende servers met verschillende operating systems kunnen draaien. Op dezelfde hardware kan bijvoorbeeld Windows en Linux als operating system worden gebruikt. Voor de gebruiker van zo'n virtuele server is dit niet anders dan een niet-virtuele server. De virtualisatie wordt gedaan door virtualisatiesoftware die tussen de daadwerkelijk hardware en het operating system draait.

52 Daarbij zijn sommige servers automatisch afgesloten, anderen zijn handmatig door de systeembeheerder uitgezet. Zie bijlage D voor meer informatie hierover. Bijlage D is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

Oorzaak ICT-uitval

De ICT-uitval in het IJsselland Ziekenhuis begon kort voor 01:30 uur met een netwerkstoring van ongeveer vijf minuten. Door deze storing werd een groot aantal (virtuele) servers uitgeschakeld. Dit zorgde ervoor dat de applicaties die op deze servers draaiden niet meer bereikbaar waren voor de gebruikers. Daardoor viel een belangrijk deel van de ICT-voorzieningen in het ziekenhuis weg. Gedurende het voorval is niet duidelijk geworden wat de oorzaak was van de netwerkstoring. Pas achteraf, na analyse van de logfiles door het ziekenhuis en de (externe) netwerkbeheerder, werd duidelijk dat de storing werd veroorzaakt door een automatische herconfiguratie van het netwerk. Gedurende deze zogenoemde *topology change*, die ongeveer vijf minuten duurde, was het netwerk niet beschikbaar. Daarna was het netwerk weer beschikbaar voor de gebruikers. Ondanks dat de *topology change* maar vijf minuten duurde, heeft het automatisch en handmatig uitschakelen van (virtuele) servers, en de onduidelijkheid die daarna ontstond over de status van de netwerkstoring, ervoor gezorgd dat de gevolgen van deze storing pas na twaalf uur waren verholpen.

Het ziekenhuis en de (externe) netwerkbeheerder hadden achteraf elk een eigen verklaring voor de oorzaak van de *topology change* in het netwerk. De Raad kan op basis van zijn onderzoek niet met zekerheid vaststellen wat de daadwerkelijke oorzaak van deze *topology change* was. Dit als gevolg van een beperkte mate van registratie (*logging*) van gebeurtenissen (*events*) in het netwerk door het IJsselland Ziekenhuis. Er is daarmee te weinig informatie bewaard gebleven om de achterliggende oorzaak van de storing met zekerheid te kunnen vaststellen.[53]

Incidentbestrijding

Om 01:25 uur werd de dienstdoende systeembeheerder door de receptie op de hoogte gebracht van een storing in de telefonie en het ziekenhuisinformatiesysteem (ZIS).[54] De systeembeheerder voerde een aantal testen uit op het systeem en constateerde dat er een netwerkstoring was geweest en dat een aantal applicatieservers onbereikbaar was. Hij meldde dit om 01:55 uur bij een medewerker van de externe netwerkbeheerder van het ziekenhuis. Samen constateerden ze dat het netwerk op dat moment functioneerde, maar dat het wel traag was. Vervolgens gingen het ziekenhuis en de externe netwerkbeheerder ieder onafhankelijk van elkaar op zoek naar de oorzaak van het probleem. Dit werd bemoeilijkt doordat de systemen in het ICT-fundament van het ziekenhuis beperkt bewaakt (gemonitord) werden. Daardoor ontving de systeembeheerder van het ziekenhuis geen (geautomatiseerde) meldingen over welke servers of applicaties last hadden, en er waren ook geen meldingen van de netwerkapparaten zelf.

Om de ICT-voorzieningen in het ziekenhuis weer te laten functioneren, dienden alle uitgeschakelde applicatieservers weer opgestart te worden. De systeembeheerder van het IJsselland Ziekenhuis vond het, met het oog op het risico van dataverlies, niet verantwoord om de servers weer op te starten zonder dat hiervoor groen licht werd

53 In bijlage D worden twee mogelijke, achterliggende oorzaken besproken.
54 Het IJsselland Ziekenhuis beschikte op het moment van de storing nog niet over een elektronisch patiëntendossier, maar maakt gebruik van een voorloper, het ziekenhuisinformatiesysteem (ZIS) van de leverancier SAP.

gegeven door de netwerkbeheerder. Hij was daarbij in de veronderstelling dat de beheerder contact op zou nemen als de oorzaak van de storing bekend was, waarna de applicatieservers weer opgestart konden worden. De externe netwerkbeheerder was hiervan echter niet op de hoogte en was op zijn beurt in de veronderstelling dat het IJsselland Ziekenhuis op dat moment geen ondersteuning meer nodig had, omdat het netwerk weer functioneerde. Door deze miscommunicatie duurde het de rest van de nacht, tot ongeveer 06:30 uur, voordat gezamenlijk werd besloten dat het verantwoord was om de uitgeschakelde applicatieservers weer op te starten. Dit nam op zichzelf vervolgens weer een aantal uur in beslag. Om 13:30 uur waren de ICT-voorzieningen in het ziekenhuis weer volledig operationeel.

Crisisbeheersing
Kort na het optreden van de storing werd het dienstdoende nachthoofd hierover geïnformeerd door de receptie van het ziekenhuis. Het nachthoofd besloot na een gesprek met de dienstdoende systeembeheerder om alle noodprocedures te starten, ook voor alle systemen die wel leken te werken. Ook werden de kernleden van het crisisteam (de dienstdoende crisiscoördinator, de voorzitter van de raad van bestuur en het hoofd bedrijfshulpverlening) geïnformeerd. Deze kernleden van het crisisteam besloten na een kort telefonisch overleg, dat het instellen van de noodprocedures door het nachthoofd voor dat moment voldoende was. Het eerste kritieke moment voor de veiligheid van patiënten zou volgens hen rond 08:00 uur ontstaan bij de medicijnronde. De voorzitter van de raad van bestuur bepaalde daarom dat de kernleden van het crisisteam om 06:00 uur in het ziekenhuis bij elkaar zouden komen om de situatie te bespreken en passende maatregelen te treffen.

Tijdens het overleg om 06:00 uur was nog niet duidelijk wanneer de ICT-systemen weer hersteld zouden zijn en werd besloten alle dienstdoende artsen op te roepen voor een volgende bijeenkomst om 07:00 uur. In dat overleg werd met de dienstdoende artsen besproken bij welke patiënten en afdelingen problemen zouden kunnen ontstaan en welke maatregelen nodig waren om de veiligheid en continuïteit van zorg te kunnen garanderen. Hierbij werd besloten tot een opnamestop, omdat het leveren van goede zorg voor patiënten volgens de aanwezigen anders niet meer gegarandeerd kon worden. Ook werd besloten een aantal patiënten te verplaatsen en/of verscherpt te monitoren. Aansluitend op het overleg beoordeelden artsen met de afdelingsverpleegkundigen de medicijnverstrekking van alle patiënten om een veilige medicijnuitgifte van 08:00 uur mogelijk te maken. Daarnaast beoordeelden zij gelijktijdig de situatie van de patiënten en de continuïteit van zorg op de afdelingen om zeker te stellen dat er met de afgekondigde maatregelen ook de komende uren verantwoorde zorg kon worden geleverd.

In de daaropvolgende uren veranderde er weinig aan de situatie in het ziekenhuis. Om 10:45 uur werd het de crisisorganisatie duidelijk dat men reeds vergevorderd was met het weer opstarten van de systemen. Besloten werd om vooralsnog de huidige werkwijze en opnamestop in stand te houden totdat er meer zekerheid was over de stabiliteit en integriteit van de systemen. Toen om 12:30 uur bleek dat de medische systemen weer grotendeels in bedrijf waren, werd besloten tot een gefaseerde en begeleide opstart van de OK en SEH. Om 13:00 uur werd het crisisteam opgeheven en om 13:30 uur waren de ICT-voorzieningen in het ziekenhuis weer volledig operationeel.

3.1.3 Dijklander Ziekenhuis

Op maandag 16 juli 2018 viel in het Dijklander Ziekenhuis in Hoorn om 16:00 uur de toegang tot de storage weg. Door de storing hadden de artsen in het ziekenhuis geen toegang meer tot de elektronische patiëntendossiers, reden waarom rond 16:30 uur werd besloten de SEH te sluiten. Later werden ook de verloskamer en de hartbewaking gesloten. Na twee uur en drie kwartier was het EPD weer beschikbaar voor de kritische afdelingen. Toen de volgende ochtend om 08:00 uur een defect hardwarecomponent van één van de servers werd vervangen, konden de overige ICT-systemen weer geleidelijk opgestart en belast worden. Uiteindelijk functioneerde de ICT-systemen weer volledig om 14:00 uur. De ICT-storing heeft daarmee in totaal ongeveer 22 uur geduurd.

Oorzaak ICT-uitval

Op 16 juli 2018 werd de vloer in de serverruimte van het Dijklander Ziekenhuis in Hoorn opgehoogd om de servers beter te kunnen koelen. Om 12:30 uur, op het moment dat het ziekenhuis in vol bedrijf was, werd met het werk gestart. Bij de werkzaamheden werden de serverkasten, met draaiende apparatuur, door een gespecialiseerd bedrijf omhoog gehesen om aan de vloer eronder te werken. Hierbij raakte rond 14:15 uur de controller van de primaire storageserver defect.[55] Dit defect is waarschijnlijk[56] het gevolg van het kantelen van de serverkast waar de server inzat. Als reactie op het defect schakelde de storageserver automatisch over naar een secundaire storageserver, die zich in een andere serverruimte bevond. Dit ging zonder problemen, waardoor in eerste instantie niemand hier iets van merkte.

Een storagespecialist[57] van het ziekenhuis werd door een automatisch gegenereerde mail op de hoogte gesteld van de overschakeling van de storage naar het redundante systeem. In overleg met zijn collega[58], de voor de storage verantwoordelijke systeembeheerder, ging hij direct op zoek naar de oorzaak hiervan, maar kon deze niet vinden. De storagespecialist vond wel dat de belasting van de secundaire storageserver aan de hoge kant was. Om te voorkomen dat de ICT-voorzieningen in het ziekenhuis hierdoor minder goed zouden gaan functioneren, besloot hij kort voor 16:00 uur om de storage geforceerd[59] terug te schakelen naar de primaire storageserver. Aangezien deze server defect was, lukte dit niet en viel de storage uit met uitval van ICT-voorzieningen in het ziekenhuis tot gevolg.

Incidentbestrijding

Na de uitval van de storage gingen ICT-medewerkers van het ziekenhuis direct op zoek naar de oorzaak van de problemen, daarin telefonisch ondersteund door een ingeschakelde externe onderhoudspartij.[60] Omstreeks 17:00 uur kwamen ze tot de conclusie dat de controller van de primaire storageserver kapot was. Hierop zetten ze de

55 Het moederbord van de controller begaf het.
56 De Raad heeft deze causaliteit niet onomstotelijk kunnen vaststellen, maar acht dit wel zeer aannemelijk.
57 Dit is een medewerker van de ICT-afdeling die zich vooral bezighoudt met de dataopslag van een organisatie.
58 Deze collega was op dat moment op de andere ziekenhuislocatie in Purmerend aan het werk.
59 Dit betekent dat een commando werd gegeven dat alleen door een handmatig ingevoerd commando, en dus niet door het systeem zelf, weer ongedaan kon worden gemaakt.
60 Deze onderhoudspartij was op dat moment niet verantwoordelijk voor de storageservers van het ziekenhuis, omdat het contract met hen pas later in zou gaan. Het ziekenhuis schakelde deze onderhoudspartij in eerste instantie (per abuis) toch in voor ondersteuning.

storage terug naar de secundaire storageserver, wat zorgde voor herstel van de storage. Daarop kwam een beperkt aantal ICT-voorzieningen in het ziekenhuis weer beschikbaar. Pas na het herstarten van alle applicatieservers die gebruik maken van de storage, zouden alle ICT-voorzieningen in het ziekenhuis weer beschikbaar zijn. Het systeem startte echter maar langzaam op en er waren zorgen over de belastbaarheid van het systeem, omdat de controller van de primaire storageserver nog steeds defect was. Naar aanleiding van deze zorgen werd besloten om het gebruik van het systeem te beperken tot honderd werkplekken totdat de defecte controller zou zijn vervangen.

Nadat de verbinding met de secundaire storageserver was hersteld, ging de verantwoordelijke externe onderhoudspartij[61] op zoek naar een oplossing voor het probleem. Het lukte hen echter niet om toegang te krijgen tot het systeem, waarop om 17:58 uur de fabrikant van het storagesysteem met hoge prioritering werd ingeschakeld. Deze kwam er rond 23:00 uur achter dat het moederboard van de controller defect was. Een aantal uur later, om 04:00 uur, arriveerde een monteur met een vervangend moederbord om de defecte controller te repareren. Dit ging minder voorspoedig dan gedacht, doordat het systeem niet up-to-date bleek en rommelige bekabeling op orde moest worden gebracht. Hierdoor duurde het uiteindelijk ongeveer vier uur om de defecte controller te vervangen. Weer een paar uur later, op 17 juli rond 11:45 uur, was de storage weer volledig operationeel en na het opstarten[62] van alle systemen was de storing om 14:00 uur opgelost.

Crisisbeheersing
Op het moment dat de storage uitviel, om 16:00 uur, merkten de meeste medewerkers in het ziekenhuis dat meteen. Zo ook de dienstdoende crisiscoördinator, die kort daarop besloot het operationeel crisisteam bij elkaar te roepen. Tijdens de eerste vergadering om 16:30 uur bleek dat het om een grootschalige storing ging, waarop de crisiscoördinator besloot om de crisisorganisatie op te schalen naar het crisisbeleidsteam. Doordat zowel het EPD als het nood-EPD[63], dat juist in dat soort situaties zou moeten werken, niet beschikbaar waren[64], kwam het leveren van goede zorg in het geding volgens de crisiscoördinator. Daarom besloot het crisisbeleidsteam om de instroom van nieuwe patiënten zoveel mogelijk te beperken middels een opnamestop voor de afdelingen SEH, verloskunde en hartbewaking en de OK (behoudens spoedbehandelingen) te sluiten.

Het crisisbeleidsteam was van mening dat de impact van de ICT-uitval voor de liggende patiënten beperkt was. Wel besloot het team om patiënten bij verloskunde individueel aan bed te gaan monitoren, twee patiënten direct over te plaatsen van de OK (*recovery*) naar de IC, en één patiënt direct over te plaatsen van de OK naar de verpleegafdeling. Daarnaast besloot het om extra personeel in te zetten bij verloskunde in verband met een instabiele patiënt en twee bevallingen die gaande waren. Ten slotte werd besloten enkele voor de volgende dag geplande operaties uit te stellen.

61 Inmiddels was duidelijk dat een andere onderhoudspartij verantwoordelijk was voor de storageservers van het ziekenhuis, waarop die werd ingeschakeld.
62 Inclusief synchronisatie en doortesten van de integriteit van de data van alle systemen.
63 Dit is een gesynchroniseerde leesversie van het EPD.
64 Dit kwam doordat de toegang tot het nood-EPD via de defecte storageserver verliep.

In de loop van de avond, na terugschakeling naar de secundaire storageserver, was weer beperkt toegang mogelijk tot patiëntgegevens via het EPD. Naar oordeel van het ziekenhuis kon de avond medicijnverstrekking verantwoord plaatsvinden en was het volgens het crisisbeleidsteam niet nodig om alle dienstdoende artsen naar het ziekenhuis te laten komen. In afwachting van de reparatie van de controller werd daarnaast besloten om het gebruik van het systeem te beperken tot honderd werkplekken. Ook werd besloten om alle relevante patiënt- en medicatiegegevens voor de volgende dag uit te laten printen om bij falen van de reparatie nog verantwoorde zorg te kunnen blijven leveren.

De volgende ochtend om 08:15 uur hoorde het crisisteam van de afdeling ICT dat de reparatie van de storageserver geslaagd was, maar dat het opnieuw opstarten[65] van alle systemen nog de hele ochtend voor problemen zou kunnen zorgen. Deze problemen deden zich inderdaad voor, wat het ziekenhuis noopte om verschillende operaties voor die ochtend uit te stellen. Rond 11:00 uur stelde het crisisbeleidsteam vast dat het systeem weer stabiel was, waarna de opnamestop vanaf 12:00 uur werd opgeheven. Om 14:00 uur was de storing volledig opgelost.

3.1.4 Samenvattende conclusie

Voor de drie onderzochte voorvallen zijn verschillende (directe) oorzaken aan te wijzen. Het blijkt bovendien dat relatief kleine storingen eenvoudig, en soms onnodig, kunnen uitmonden in grootschalige uitval van ICT.

3.2 Voorvaloverstijgende factoren

De Raad heeft de drie voorvallen die centraal staan in dit onderzoek uitgebreid geanalyseerd. Daarbij komen diverse onvolkomenheden naar voren die zich elk bij minimaal twee ziekenhuizen hebben voorgedaan. Deze zogenoemde voorvaloverstijgende factoren bieden op operationeel niveau inzicht in de tekortkomingen in het beheersen van risico's ter voorkoming van ICT-uitval en in het beperken van de gevolgen hiervan voor de patiëntveiligheid. De voorvaloverstijgende factoren worden hieronder in kaart gebracht.

3.2.1 Inrichting en beheer ICT-fundament niet op orde

Een eerste voorvaloverstijgende factor is de inrichting en het beheer van het ICT-fundament. Dit heeft een belangrijke rol gespeeld bij zowel het ontstaan als de bestrijding van de ICT-uitval. In het vervolg van deze paragraaf komen de verschillende deelonderwerpen die hiermee samenhangen aan bod.

Redundante systemen niet (afdoende) ingericht

Alle drie de onderzochte ziekenhuizen beschikten over redundante systemen, die als achtervang fungeren voor het geval er een storing optreedt in (een aantal van) de meest

65 Inclusief synchronisatie en doortesten van de integriteit van de data van alle systemen.

kritische elementen van het ICT-fundament. De voorvallen laten zien dat de aanwezigheid van redundante systemen op zichzelf onvoldoende voorwaarde is om ICT-uitval te voorkomen. Andere factoren, zoals keuzes over de inrichting en het beheer van redundante systemen, alsmede de afstemming tussen partijen en de rol van menselijk handelen, kunnen het adequaat functioneren van redundante systemen ondermijnen.

Het voorval in het Radboudumc is hier een goede illustratie van. Daar had het storagesysteem de functionaliteit om geografisch redundant te worden ingericht, maar was dit op het moment van het voorval nog niet volledig gebeurd.[66] Ook bij het Dijklander Ziekenhuis speelden redundante systemen een rol bij het voorval. Daar werkte de redundantie in het storagesysteem in eerste instantie goed: zodra het defect aan de ene storageserver optrad, schakelde het systeem automatisch over naar de andere storageserver zonder dat gebruikers dit merkten. Doordat het systeem kort daarna handmatig werd teruggeschakeld van de secundaire storageserver naar de primaire server, leidde de storing in de primaire server toch tot een grootschalige ICT-uitval. Op het moment dat de ICT uitviel, bleek dat het back-upsysteem van het EPD, het nood-EPD, niet goed ingericht was. De toegang daartoe liep namelijk ook via het storagesysteem en kon dus niet gebruikt worden op het moment dat dit nodig was.[67]

Redundante systemen moeten, zoals de voorvallen laten zien, zodanig zijn ingericht dat ze bij ICT-uitval ook daadwerkelijk in werking treden. Procedures dienen dermate duidelijk te zijn ingericht dat het gevaar op menselijke fouten tot een minimum beperkt wordt. Het periodiek en in samenhang testen van redundante voorzieningen is cruciaal voor een adequate voorbereiding op ICT-uitval. Het IJsselland Ziekenhuis en het Dijklander Ziekenhuis geven aan dat zij redundante voorzieningen op individueel niveau (storage, HiX-database cluster) testen, maar het niet aandurven een hele Main Equipment Room (MER)[68] uit te schakelen, omdat niet duidelijk is tot welke gevolgen dat zou kunnen leiden. Daarmee worden de individuele voorzieningen niet in samenhang getest. Dat in het Dijklander Ziekenhuis het nood-EPD onverwacht niet beschikbaar was, laat zien dat een test van zo'n geïntegreerde omgeving toegevoegde waarde heeft. Het niet-testen van ICT-voorzieningen met het oog op ICT-uitval is opmerkelijk vanwege de hoge mate van afhankelijkheid van ICT en omdat diverse normen de periodieke beproeving en evaluatie van noodvoorzieningen en -procedures verplicht stellen.[69] Bovendien blijken de onderzochte ziekenhuizen dit soort testen wel te doen voor uitval van de elektriciteitsvoorziening.

Beperkte monitoring van systemen

Hoewel bij alle drie de onderzochte ziekenhuizen ICT-systemen op enigerlei wijze gemonitord werden, was er niet in alle gevallen sprake van voldoende *realtime* en continue monitoring. Vooral bij het voorval in het IJsselland Ziekenhuis heeft het ontbreken van voldoende *realtime* en continue monitoring van systemen een belangrijke

66 Zie voor een uitgebreide beschrijving van dit deel van de analyse van het voorval in het Radboudumc bijlage D.1. Deze bijlage is te vinden op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl

67 Zie voor uitgebreide beschrijving van dit deel van de analyse van het voorval in het Dijklander Ziekenhuis bijlage D.3.

68 Een ruimte waarin centrale ICT-apparatuur is opgesteld.

69 Onder andere NEN 7510 en NEN 7512. Ook het VMS vraagt dat noodvoorzieningen en procedures getest worden.

rol gespeeld. Hierdoor werd de netwerkstoring niet (voor)tijdig gesignaleerd en kon de directe oorzaak van het incident niet achterhaald worden. Dit heeft een snelle oplossing van het incident in de weg gestaan. Het ontbreken van informatie over de storing heeft er daarnaast toe bijgedragen dat tot op heden geen duidelijkheid is over de achterliggende oorzaak van het incident. Dit staat het treffen van de juiste maatregelen ter voorkoming van toekomstige incidenten in de weg.[70]

Tekortkomingen in invulling regierol richting externe partijen
In de analyse van de voorvallen kwam het belang van het goed invullen van de regierol naar voren. Dit betreft de aansturing van externe partijen door ICT-afdelingen van de onderzochte ziekenhuizen. Bij het IJsselland Ziekenhuis waren bijvoorbeeld de rollen en wederzijdse verantwoordelijkheden tussen het IJsselland Ziekenhuis en de externe netwerkbeheerder ontoereikend gedefinieerd en beschreven. Dit heeft eraan bijgedragen dat een fout in de configuratie niet eerder werd opgemerkt en gerepareerd. Deze foutieve configuratie is één van de twee mogelijke oorzaken voor het ontstaan van de ICT-uitval in het ziekenhuis.[71]

Ook bij het bestrijden van ICT-storingen is een goede invulling van de regierol van belang, omdat het onduidelijkheid kan voorkomen over wie verantwoordelijk is om het probleem op te lossen en welke afspraken daarbij gelden over respons- en reparatietijden. De gevolgen van het niet goed invullen van de regierol voor het bestrijden van een ICT-storing kunnen geïllustreerd worden aan de hand van het voorval in het Dijklander Ziekenhuis. Daar werd in eerste instantie de verkeerde onderhoudspartij ingeschakeld, omdat het voor de betreffende medewerker niet duidelijk was welke partij op dat moment verantwoordelijk was voor het beheer en onderhoud van het systeem. Ook moest een onderdeel vervangen worden om de storing op te kunnen lossen. Om een snelle oplossing te bewerkstelligen, had het ziekenhuis dit onderdeel zelf op voorraad moeten hebben of had het bij de onderhoudspartij op voorraad moeten zijn. Dat was niet het geval. Deze problemen in de bestrijding van het incident zorgden ervoor dat de incidentbestrijding langer duurde dan nodig.[72] Betere afstemming tussen ziekenhuizen en externe organisaties zoals onderhoudspartijen, kan dit soort situaties voorkomen.

Onvoldoende inrichting van change- en incident management
Goed *change management* en *incident management* draagt bij aan het voorkomen van langdurige ICT-uitval. *Change management* is erop gericht om wijzigingen in het ICT-landschap (onderhoud en/of vernieuwing) op een beheerste manier door te voeren, met als doel om onverwachte storingen als gevolg van wijzigingen te voorkomen. *Incident management* is erop gericht om ICT-incidenten op een gestructureerde manier te bestrijden, zodat wordt voorkomen dat medewerkers ad hoc te werk gaan en daarmee mogelijk het incident eerder verergeren dan oplossen.

70 Zie voor een uitgebreide beschrijving van dit deel van de analyse van het voorval in het IJsselland Ziekenhuis bijlage D.2. Deze bijlage is te vinden op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl
71 Zie voor een uitgebreide beschrijving van dit deel van de analyse van het voorval in het IJsselland Ziekenhuis bijlage D.2. Deze bijlage is te vinden op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl
72 Zie voor een uitgebreide beschrijving van dit deel van de analyse van het voorval in het Dijklander Ziekenhuis bijlage D.3. Deze bijlage is te vinden op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl

De ICT-uitval in het Dijklander Ziekenhuis laat het belang van *change management* en *incident management* zien. Daar werden de werkzaamheden in de serverruimte van het ziekenhuis niet voorbereid als een ICT-wijziging conform *changemanagement procedures*. Zo was er geen draaiboek voor de ICT-werkzaamheden, was er geen toezicht op de werkzaamheden en was er geen plan van aanpak in het geval dat één of meerdere servers zou(den) uitvallen. Daardoor kon het gebeuren dat een ICT-medewerker geconfronteerd werd met het incident (de overschakeling van de storage naar de secundaire server) zonder dat hij wist wat de werkzaamheden precies inhielden. Bij het bestrijden van het incident kon deze medewerker niet terugvallen op een incidentbestrijdingsprocedure en er waren ook geen afspraken over het escaleren naar het management van de ICT-afdeling of naar de crisisorganisatie.[73]

3.2.2 Beperkte voorbereiding op ICT-uitval

Een tweede voorvaloverstijgende factor is de voorbereiding op ICT-uitval. Uit het onderzoek naar de voorvallen komt naar voren dat de onderzochte ziekenhuizen beperkt voorbereid waren op ICT-uitval. Een eerste aspect hierbij is de planvorming. Waar de onderzochte ziekenhuizen allen beschikten over een uitgewerkte, algemene voorbereiding op calamiteiten en crises, ontbraken concrete plannen rondom het risico van ICT-uitval. Het Radboudumc beschikte bijvoorbeeld niet over een concrete uitwerking van dit risico, ondanks dat het als één van de belangrijkste risico's was aangemerkt in het crisisplan. In dat plan was aangegeven dat de belangrijkste risico's verder zouden worden uitgewerkt. Het Radboudumc beschikte wel over een zogenaamde scenariokaart voor dit risico, die de crisisorganisatie in algemene termen aandachtspunten geeft over hoe te handelen in de warme fase bij het optreden van dit risico. Dit is echter geen plan dat de crisisorganisatie concreet voorbereidt op dit risico en hoe dit het beste kan worden bestreden in het Radboudumc. Ook het IJsselland Ziekenhuis en het Dijklander Ziekenhuis beschikten niet over dergelijke plannen.

Naast voorbereiding door middel van (crisis)plannen is het van belang crisisfunctionarissen met opleiding en training te prepareren op ICT-uitval. In de onderzochte ziekenhuizen was daarin niet voorzien. Ook werd niet geoefend met een scenario waarbij sprake is van een grootschalige uitval van ICT, terwijl juist dit soort oefeningen verbeterpunten in het systeem kunnen blootleggen. Dat de noodcommunicatie bij ICT-uitval niet werkt, zoals in het Radboudumc het geval was, komt bij uitstek naar voren bij een oefening. Ook was het laboratorium voorafgaand aan de crisis niet in beeld als kritisch proces, maar bleek dat tijdens de crisis wel te worden. Ook het ontbreken van een informatiemanagementprocedure in de crisisorganisatie wordt bij een oefening direct zichtbaar. Bij het Radboudumc leidde het ontbreken van een informatiemanagement-proces tijdens het incident tot vertraging in de beeldvorming.

3.2.3 Onvolledige evaluatie en beperkt onderzoek naar oorzaak storing

Een laatste voorvaloverstijgende factor die naar voren komt uit de analyse van de voorvallen is het leren van ICT-uitval. Aan de basis van leren van voorvallen ligt het evalueren ervan. Een evaluatie van voorvallen geeft inzicht in de (achterliggende)

73 Zie voor een uitgebreide beschrijving van dit deel van de analyse van het voorval in het Dijklander Ziekenhuis bijlage D.3. Deze bijlage is te vinden op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl

oorzaken op basis waarvan maatregelen genomen kunnen worden om een soortgelijk voorval in de toekomst te voorkomen. Het belang van evalueren en leren wordt door de onderzochte ziekenhuizen onderkend. Alle drie de ziekenhuizen hebben de voorvallen geëvalueerd, zij het met een beperkte focus en vraagstelling. Zo zijn de gevolgen voor de patiëntveiligheid onderbelicht gebleven. De betrokken ziekenhuizen hebben niet gestructureerd en diepgaand geïnventariseerd welke (kans op) schade er voor patiënten is ontstaan als gevolg van ICT-uitval. Daardoor blijft ongewis wat de effecten van ICT-uitval op patiëntveiligheid zijn.[74] Op technisch niveau is niet in alle gevallen de oorzaak van de storing aan het licht gekomen, mede door een beperkte vastlegging van data. Dit belemmert het doen van grondig onderzoek naar de directe en achterliggende oorzaken van de storing, het treffen van adequate beheersmaatregelen, en daarmee het voorkomen van soortgelijke incidenten in de toekomst.

Om daadwerkelijk te kunnen leren van ICT-incidenten is het belangrijk dat de uitkomsten van de evaluatie en de getrokken lessen worden vastgelegd, dat deze vertaald worden naar verbetermaatregelen en dat de implementatie van de verbetermaatregelen wordt gevolgd. Bij het Radboudumc en het Dijklander Ziekenhuis heeft dit plaatsgevonden. Bij het IJsselland Ziekenhuis niet. De in dit laatste ziekenhuis geïnterviewde betrokkenen geven aan dat er geëvalueerd is, maar een evaluatieverslag is niet beschikbaar. Er is daarom ook geen gedeeld beeld van de geleerde lessen en het is onduidelijk welke leerpunten in de organisatie zijn geïmplementeerd.

3.2.4 Bevindingen bij drie andere ICT-storingen

De Onderzoeksraad merkt op dat de onderzochte voorvallen niet op zichzelf staan. De beschouwing van drie andere ICT-storingen[75] laat zien dat ook daar diverse van de hiervoor benoemde factoren een rol hebben gespeeld. Dit betreft met name onvolkomenheden in het ICT-beheer, zoals het uitvoeren van software-updates en de borging van de continuïteit van de (ICT-)dienstverlening. Ook blijkt bij meerdere van deze voorvallen zowel de monitoring van systemen als de afstemming tussen het ziekenhuis en externe partijen een aandachtspunt. Dit laatste speelde bijvoorbeeld een rol bij de technische incidentbestrijding in het Amsterdam UMC (locatie VUmc), bij het oplossen van het probleem met het Verpleegkundig- en Medisch Oproepsysteem in het Medisch Spectrum Twente en bij het ontstaan van de storing in de Noordwest Ziekenhuisgroep.

Daarnaast spelen ook bij deze incidenten tekortkomingen in de voorbereiding op de ICT-uitval een rol. Dit wordt bijvoorbeeld geïllustreerd door het voorval in het Medisch Spectrum Twente, waarbij tijdens het incident bleek dat de sloten van de apparatuurkasten afhankelijk waren gemaakt van het netwerk en men over het hoofd zag dat er een noodcentrale voor telefonie was. Door planvorming en activiteiten op het terrein van opleiden, trainen en oefenen, kunnen dergelijke problemen mogelijk voorafgaand aan een storing aan het licht komen.

74 In hoofdstuk 4 wordt hier uitgebreider bij stilgestaan.

75 Het gaat om ICT-storingen in het Amsterdam UMC, locatie VUmc, de Noordwest Ziekenhuisgroep en Medisch Spectrum Twente. De Onderzoeksraad heeft op basis van het onderzoek dat de ziekenhuizen en hun ingehuurde ICT-dienstverleners zelf hebben uitgevoerd, de voorvallen beschouwd. Op basis van deze documenten, die de Onderzoeksraad kort na de voorvallen heeft ontvangen, zijn de voorvallen beschreven. Dat de Onderzoeksraad deze beschrijving heeft opgenomen in het rapport, betekent echter niet dat de Onderzoeksraad de bevindingen en conclusies van andere partijen onderschrijft. Daarvoor is eigen onderzoek nodig.

Tot slot blijkt uit deze incidenten dat, net als bij de drie diepgaand onderzochte voorvallen, de ziekenhuizen in hun evaluaties van de incidenten nauwelijks tot geen aandacht besteed hebben aan de impact van de ICT-uitval op de patiëntveiligheid. Dit betreft zowel de aandacht voor eventuele daadwerkelijke schade als de verhoogde kans op schade voor patiënten als gevolg van de storingen.

Zie voor een uitgebreide beschrijving van de bevindingen bij de overige drie ziekenhuizen bijlage F.[76]

3.2.5 Samenvattende conclusie

Onvolkomenheden in de inrichting en het beheer van het ICT-fundament hebben een belangrijke rol gespeeld bij het ontstaan en bestrijden van de ICT-storingen in de drie onderzochte ziekenhuizen. Dit betreft met name de inrichting van redundante voorzieningen, het *realtime* en continu monitoren van het ICT-landschap, de invulling van de regierol en de inrichting van het change- en incidentmanagement. De onderzochte ziekenhuizen waren daarnaast beperkt voorbereid op ICT-uitval. Zo was er geen concrete planvorming gericht op het beheersen van de gevolgen van ICT-uitval, werd er niet geoefend met grootschalige ICT-uitvalscenario's en werden redundante voorzieningen niet in samenhang getest. Tot slot werden de voorvallen door twee van de drie ziekenhuizen beperkt geëvalueerd met betrekking tot het achterhalen van de directe en achterliggende (technische) oorzaken en brachten alle drie de ziekenhuizen de gevolgen van de ICT-uitval voor de patiëntveiligheid beperkt in kaart.

3.3 Conclusie

Een hoge beschikbaarheid van ICT-voorzieningen is in de 24/7 omgeving van ziekenhuizen, die bovendien een belangrijke maatschappelijke functie vervullen, noodzakelijk voor het waarborgen van continuïteit van zorg en de veiligheid van patiënten. Het voorkomen van ICT-uitval vereist een goede inrichting en beheer van het ICT-fundament, alsmede een goede voorbereiding op ICT-uitval en het adequaat leren van ICT-voorvallen. Deze factoren dragen niet alleen bij aan het voorkomen van storingen, maar zijn ook van belang om storingen zo snel mogelijk te kunnen verhelpen als deze zich toch voordoen. Hoewel de ziekenhuizen verschillen in de mate waarin zij aandacht hebben voor deze factoren, constateert de Onderzoeksraad dat deze factoren bij de onderzochte voorvallen hebben bijgedragen aan het langdurig uitvallen van ICT.

76 Bijlage F is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

4 PATIËNTVEILIGHEID BIJ ICT-UITVAL

In het vorige hoofdstuk is beschreven hoe de ICT-storingen bij het Radboudumc, het Dijklander Ziekenhuis en het IJsselland Ziekenhuis zijn ontstaan, hoe de incidentbestrijding is verlopen en hoe de crisisbeheersing is gegaan. In dit hoofdstuk staat de vraag centraal welke gevolgen ICT-uitval kan hebben voor de patiëntveiligheid. Om te kunnen leren van voorvallen is het belangrijk dat ziekenhuizen inzicht hebben in de wijze waarop ICT-uitval de patiëntveiligheid negatief kan beïnvloeden. In paragraaf 4.1 worden verschillende manieren in kaart gebracht waarop ICT-uitval tot (een verhoogde kans op) schade voor patiënten kan leiden. Daarbij worden tevens, aan de hand van VIM-meldingen[77] en interviews over de onderzochte voorvallen, concrete voorbeelden aangehaald. Paragraaf 4.2 laat vervolgens zien in hoeverre de onderzochte ziekenhuizen deze risico's van ICT-uitval voor de patiëntveiligheid na afloop van de voorvallen in beeld hebben gebracht. In paragraaf 4.3 worden de conclusies geformuleerd.

4.1 (Verhoogde kans op) schade voor de patiënt bij ICT-uitval

De Onderzoeksraad onderscheidt zeven manieren waarop ICT-uitval tot (een verhoogde kans op) schade aan patiënten kan leiden.[78] Van deze zeven hebben zich er zes voorgedaan bij de onderzochte voorvallen. Bij twee van deze zes manieren is dit, op basis van VIM-meldingen en interviews, uitgewerkt in een concreet voorbeeld op patiëntniveau. Deze voorbeelden zijn weergegeven in de blauwe blokken in het vervolg van deze paragraaf.

1. Patiëntinformatie niet beschikbaar

ICT-uitval kan leiden tot uitval van het EPD, waardoor er geen toegang meer is tot patiëntinformatie. In dat geval kunnen artsen en verpleegkundigen alleen nog handelen op basis van hun eigen geheugen of dat van een collega arts/verpleegkundige, op basis van informatie die de patiënt zelf kan geven, op basis van de klinische verschijnselen van de patiënt of een combinatie hiervan. Dit brengt het risico met zich mee dat mogelijk relevante informatie (allergieën, patiënthistorie, behandelalternatieven, wilsverklaringen, etc.) niet wordt meegenomen bij het vaststellen van de diagnose of behandeling. Dit kan leiden tot een beperkt beeld van de situatie en onzekerheid over behandelmogelijkheden en daarmee tot (een verhoogde kans op) schade aan de patiënt.

77 VIM staat voor Veilig Incident Melden. Hierbij worden incidenten en bijna-incidenten in ziekenhuizen gemeld, geanalyseerd en worden verbetermaatregelen voorgesteld. VIM is een methode die ontworpen is om incidenten veilig te melden, te onderzoeken en de oorzaken te categoriseren dichtbij het werkproces. Bron: Praktijkgids Veilig Incident Melden.

78 De zeven manieren waarop ICT-uitval tot (een verhoogde kans op) schade voor de patiënt kan leiden, zijn zowel gebaseerd op het onderzoek naar de ICT-storingen in het Radboudumc, het Dijklander Ziekenhuis en het IJsselland Ziekenhuis, als op de beschouwing van de ICT-storingen in het Amsterdam UMC, locatie VUmc, de Noordwest Ziekenhuisgroep en het Medisch Spectrum Twente. De Onderzoeksraad sluit niet uit dat er meer manieren zijn waarop uitval van ICT tot (een verhoogde kans op) schade aan patiënten kan leiden, zeker gezien het feit dat de digitalisering zich in hoog tempo voortzet.

In alle drie de onderzochte ziekenhuizen was de patiëntinformatie gedigitaliseerd in een informatiesysteem. In twee van de drie ziekenhuizen betrof dat een EPD, in de derde een ZIS. Het Radboudumc kampte door de ICT-uitval met beperkingen in het EPD. Het EPD was nog wel toegankelijk, maar de koppelingen met andere applicaties (zoals die van het laboratorium en de apotheek) werkten niet meer. Bij het IJsselland Ziekenhuis was het ZIS, de voorloper van het EPD, niet beschikbaar en bij het Dijklander Ziekenhuis was het gehele EPD inclusief het nood-EPD niet toegankelijk. In de loop van het voorval kwam in het Dijklander Ziekenhuis eerst het nood-EPD en daarna het EPD gedeeltelijk weer beschikbaar. Het volgende voorbeeld illustreert hoe het niet beschikbaar zijn van informatie, van invloed kan zijn op de patiëntveiligheid.

Tijdens de ICT-storing in het Dijklander Ziekenhuis werd een patiënt onwel op een algemene verpleegafdeling. De intensivist van het opgeroepen Spoed Interventie Team (SIT) had door de ICT-uitval geen actuele gegevens over de patiënt. Het team behandelde de patiënt op grond van de klinische verschijnselen die er op dat moment waren (onwelwording door bloedverlies) door toediening van extra vocht, stollingsfactoren en bloed. De bloedgroep van de patiënt kon niet gecontroleerd worden doordat het EPD en nood-EPD niet beschikbaar waren. Bij het toedienen van bloed werd het bloed niet eerst 'gekruist' met dat van de patiënt (om te controleren of het donorbloed verenigbaar is met dat van de ontvanger), maar werd gekozen voor bloed waarvan bekend is dat dit niet of nauwelijks reactie geeft. Hiermee ontstond een stabiele situatie voor de patiënt waardoor deze op de afdeling kon blijven. Hoewel deze behandeling in geval van acuut ernstig bloedverlies niet ongebruikelijk is, ontstond daarmee toch een verhoogde kans op schade ten opzichte van de situatie waarin alle gegevens over de patiënt beschikbaar zouden zijn geweest. Zo introduceerde de toediening van bloed met de gekozen bloedgroep een (beperkt) risico op een hemolytische transfusiereactie[79] en konden, door het niet-beschikbaar zijn van actuele gegevens, de risico's ten gevolge van toedienen van vocht minder goed ingeschat worden. Als het bijvoorbeeld een patiënt was geweest met hartfalen, had de extra belasting op het hart door de toegediende vloeistoffen mogelijk tot problemen kunnen leiden.

2. Opnamestop

Wanneer er sprake is van een ICT-storing, kan dit in de praktijk leiden tot het afkondigen van een opnamestop. Een dergelijke maatregel wordt in eerste instantie genomen om de zorg voor patiënten in het ziekenhuis te kunnen continueren en daarmee de veiligheid te waarborgen. Het gevolg van een opnamestop is echter tevens dat patiënten die onder normale omstandigheden voor een zorgvraag naar het betreffende ziekenhuis zouden gaan, moeten uitwijken naar een ander ziekenhuis. Dat kan leiden tot extra reistijd voor de patiënt met bijbehorende risico's voor de patiëntveiligheid. De gevolgen van een opnamestop voor de patiëntveiligheid zijn groter naarmate de reistijd naar een ander ziekenhuis langer is. Ook kan de specifieke zorg die een patiënt nodig heeft, niet altijd

79 Pamela P. Goodell, Lynne Uhl, Monique Mohammed, and Amy A. Powers. Risk of hemolytic transfusion reactions following emergency-release RBC transfusion. Am J Clin Pathol, 2010, 134:202-206.

en overal op hetzelfde niveau geleverd worden. Daarnaast kan het gebeuren dat een ander ziekenhuis niet over alle informatie over de patiënt beschikt, waardoor in acute situaties beslissingen op basis van beperkte informatie genomen moeten worden. De relevantie van deze factoren wordt met name duidelijk wanneer een ziekenhuis dat specialistische zorg levert, tot een opnamestop besluit. Het Radboudumc bijvoorbeeld, is één van de elf level-1 traumacentra in Nederland die 24/7 ernstig gewonde patiënten kan opvangen.[80] Dergelijke patiënten, die onder normale omstandigheden naar het Radboudumc worden vervoerd, moeten tijdens een opnamestop naar één van de andere tien traumacentra in Nederland worden gebracht, wat in voorkomende gevallen een aanzienlijk langere reistijd met zich kan meebrengen.

Een dergelijke situatie kan zich ook voordoen wanneer een ziekenhuis meerdere locaties heeft binnen één regio, die alle gebruik maken van centrale ICT-voorzieningen. Wanneer deze uitvallen, worden meerdere locaties getroffen en moeten patiënten uitwijken naar andere ziekenhuizen. Er zijn diverse voorbeelden van ziekenhuizen waar meerdere locaties werden geraakt en een (gedeeltelijke) opnamestop moesten afkondigen als gevolg van eenzelfde ICT-storing, zoals de storingen bij de Noordwest Ziekenhuisgroep en het Amphia Ziekenhuis, beide in 2019.

In alle drie de onderzochte ziekenhuizen werd tijdens de ICT-uitval een (gedeeltelijke) opnamestop afgekondigd, omdat het ziekenhuis de veiligheid van nieuwe patiënten niet kon waarborgen. Bij het Radboudumc werd vijf uur lang een algehele opnamestop ingesteld, het IJsselland Ziekenhuis sloot gedurende zevenenhalf uur haar deuren voor nieuwe patiënten, en het Dijklander Ziekenhuis stelde een gedeeltelijke opnamestop in die uiteindelijk negentien uur zou duren. Patiënten die (mogelijk) opgenomen moesten worden, waren voor die periode aangewezen op andere ziekenhuizen. Onderstaand voorbeeld laat zien op welke manier een opnamestop gevolgen kan hebben voor de patiëntveiligheid.

In het gebouw van het IJsselland Ziekenhuis ligt een vestiging van Huisartsenposten Rijnmond: huisartsenpost IJsselland. Na de afkondiging van de opnamestop in het ziekenhuis kreeg iemand een hartinfarct bij de huisartsenpost. Daarop is een verpleegkundige van de SEH van het ziekenhuis naar de Huisartsenpost gegaan om de patiënt te stabiliseren en te beoordelen. De patiënt kon op dat moment niet terecht in het IJsselland Ziekenhuis vanwege de sluiting van de SEH en is door een ambulance naar een ander ziekenhuis gebracht om de benodigde zorg te ontvangen.[81]

80 De traumacentra zijn voor de opvang van traumapatiënten in drie niveaus (levels) ingedeeld. Het level 3-ziekenhuis kan geïsoleerde letsels behandelen, bijvoorbeeld een enkel- of heupfractuur. In het level 2-ziekenhuis kunnen ook vitaal bedreigde patiënten worden opgevangen, maar zijn niet alle voorzieningen aanwezig, zoals neurochirurgie. In het level 1-ziekenhuis kunnen alle ernstig gewonde patiënten 24 uur per dag, 7 dagen per week worden opgevangen. Bron: https://www.lnaz.nl/trauma/levelcriteria.

81 De Onderzoeksraad heeft bij betreffende huisartsenpost navraag gedaan naar de beschreven situatie ter bevestiging van de lezing van het IJsselland Ziekenhuis. De post heeft aangegeven zonder naam van de patiënt of huisarts geen informatie te kunnen terugvinden. Het IJsselland Ziekenhuis kan binnen hun eigen systeem niet zien om welke patiënt het ging.

3. Digitale communicatiesystemen vallen weg
ICT-uitval kan leiden tot uitval van communicatiesystemen, waardoor de mogelijkheden om patiëntgegevens uit te wisselen tussen afdelingen en medewerkers onderling worden beperkt. Ook wordt de crisisbeheersing in het ziekenhuis bemoeilijkt. Zo waren in alle drie de onderzochte ziekenhuizen telefonie en intranet niet of in beperkte mate beschikbaar en werkten ook de, voor zover ingerichte en gebruikte, noodcommunicatiemiddelen niet. Dit leidde tot beperkingen in de informatieoverdracht en ruis in de crisiscommunicatie. Dit kan leiden tot misverstanden en onduidelijkheden, die ook risico's voor de patiëntveiligheid kunnen introduceren.

In twee van de drie ziekenhuizen viel als gevolg van de ICT-storing een alarm-oproepsysteem uit. Daarbij kan onderscheid worden gemaakt tussen het VOS[82], waarmee de patiënt (of iemand anders) de verpleegkundige kan alarmeren, en het Medisch Oproepsysteem (MOS)[83], waarbij alarmmeldingen van bewakingsmonitoren worden doorgegeven. Het uitvallen van deze systemen heeft impact op de patiëntveiligheid omdat de arts of verpleegkundige in geval van nood niet kan worden gealarmeerd. De gevolgen van de uitval van een VOS voor de patiëntveiligheid kunnen worden geïllustreerd aan de hand van het volgende voorbeeld.

Op het moment dat de patiënt van het eerdere voorbeeld uit het Dijklander Ziekenhuis onwel werd (zie het voorbeeld onder punt 1), kon er middels het VOS geen signalering uitgezonden worden via de mobiele telefoons als gevolg van de ICT-storing. Ook de telefonie werkte in aanvang niet goed als gevolg van de storing, wat de situatie nog lastiger maakte. Wel werkte de signalering op de kamerlamp. Het risico bestond dat de patiënt niet tijdig de zorg zou ontvangen die nodig was. In voorliggende situatie schakelde de verpleegkundige van de afdeling, die afkwam op de signalering via de kamerlamp. een collega-verpleegkundige in die een arts-assistent haalde. Deze heeft vervolgens het SIT gewaarschuwd om de patiënt te stabiliseren. Doordat het SIT snel ter plekke was, kon de patiënt toch snel geholpen worden. Hoewel dit voorval goed is afgelopen, laat dit voorbeeld zien dat het wegvallen van communicatiesystemen kan leiden tot vertraging in het geven van benodigde zorg. Daarmee kan (een verhoogde kans op) schade optreden voor de patiënt.

4. Werken op papier
Door ICT-uitval worden de positieve effecten van reeds toegepaste ICT-ontwikkelingen op de patiëntveiligheid in veel gevallen teniet gedaan. Dit speelt in belangrijke mate op het moment dat afdelingen moeten terugvallen op het registreren van

82 De basis van het VOS bestond voorheen uit een drukknop bij het bed, waarmee een lamp boven de deur kon worden bediend. Tegenwoordig zorgt de drukknop ervoor dat er een digitaal bericht over het netwerk naar de verpleegkundige wordt gestuurd, die dit bericht op zijn of haar mobiele telefoon ontvangt. De verpleegkundige kan vervolgens door middel van een telefoonverbinding direct en op afstand contact met de patiënt te hebben.

83 Het MOS werkt op hoofdlijnen hetzelfde als het VOS, met als verschil dat het alarm getriggerd wordt door apparatuur (bijv. infuuspomp of hartbewakingsmonitor) in plaats van door de patiënt. Een belangrijke nieuwe ontwikkeling op dit gebied is de 'stille IC', waarbij de bewakingsapparaten niet piepen en knipperen bij het bed van de patiënt, maar het alarm digitaal via het netwerk naar de bewakingspost sturen.

patiëntinformatie in papieren dossiers. De risico's voor de patiëntveiligheid van het werken op papier, die waren gemitigeerd door de digitalisering van patiëntinformatie, worden op dat moment geherintroduceerd. Hierbij kan gedacht worden aan het zoekraken van informatie, het verkeerd interpreteren van informatie (bijvoorbeeld door een onleesbaar handschrift) of het ontbreken van controles op juiste invoer van data (zoals in het EPD wel gebeurt). Een ander risico is dat het handmatig invoeren van informatie in digitale systemen na afloop van de storing foutgevoelig is, hetgeen kan leiden tot niet-betrouwbare patiëntinformatie (aantasting van data-integriteit). Daarbij kan ook gekozen worden om, uit kostenoverwegingen, de nieuwe gegevens wel te bewaren maar niet in het EPD in te voeren. Afhankelijk van de keuzes die hierin gemaakt worden, wordt de kans op het werken met onvolledige of foutieve patiëntinformatie, tijdens en na afloop van de storing versterkt, hetgeen ten koste gaat van de patiëntveiligheid.

Bij alle drie de onderzochte ziekenhuizen zijn meerdere afdelingen overgeschakeld op noodprocedures, wat in de praktijk betekent dat gewerkt moest worden op papier. Zo moesten in het IJsselland Ziekenhuis alle receptmutaties door assistenten van de apotheek handmatig overgeschreven worden. In het Radboudumc moesten alle aanvragen voor laboratoriumonderzoeken op papieren aanvraagformulieren ingevuld worden in plaats van digitaal via het EPD. De uitslagen van de onderzoeken moesten vervolgens door de medewerkers van het laboratorium vanuit de apparatuur overgenomen worden op papier en doorgebeld worden naar de arts die het onderzoek aan had gevraagd. Bij al deze voorbeelden is de kans dat er fouten optreden groter dan in het gedigitaliseerde proces.

5. Terugval in efficiëntie
Het overschakelen op noodprocedures tijdens ICT-uitval betekent niet alleen dat er een grotere kans op fouten in het proces sluipt, maar ook dat het proces minder efficiënt wordt. De efficiëntie die door automatisering in het proces wordt aangebracht, valt namelijk weg zodra ICT uitvalt. De tijdigheid van zorg, een belangrijke voorwaarde voor het verlenen van goede zorg, kan hierdoor in het geding komen. Dat kan leiden tot een (verhoogde kans op) schade voor de patiënt. Het moment van de ICT-uitval en de duur ervan spelen een belangrijke rol bij de mate waarin dit gevolgen kan hebben voor de patiëntveiligheid. In de nacht en in het weekend is een terugval in efficiëntie over het algemeen beter op te vangen dan op weekdagen overdag, omdat het dan rustiger is in het ziekenhuis. Ook is het werken volgens noodprocedures voor een klein aantal uur nog goed vol te houden, maar niet wanneer sprake is van langdurige ICT-uitval (zie ook punt 6 van deze paragraaf).

Bij alle drie de voorvallen is er een terugval in efficiëntie van de zorgprocessen geweest doordat afdelingen moesten overschakelen op noodprocedures. Een voorbeeld van de manier waarop ICT-uitval doorwerkt in een terugval van efficiëntie, zijn de problemen bij het laboratorium van het Radboudumc. Doordat daar op papier gewerkt moest worden, was er een sterke terugval in efficiëntie. Waar normaal tijdens piekmomenten ongeveer duizend monsters per uur geanalyseerd kunnen worden, kon het laboratorium nu alleen nog spoedaanvragen verwerken. Na verloop van tijd werd het ook steeds moeilijker om de spoedaanvragen tijdig te verwerken. Daarom werd de crisisorganisatie gevraagd een opnamestop in te voeren, die uiteindelijk vijf uur duurde. Dit voorbeeld laat zien dat de terugval in efficiency niet alleen gevolgen kan hebben voor de patiëntveiligheid doordat

de tijdigheid van zorg in het geding kan komen, maar ook doordat het kan leiden tot een opnamestop (zie punt 2 van deze paragraaf).

6. Vermoeidheid van mensen
De terugval in efficiëntie van processen tijdens de voorvallen heeft uiteindelijk ook gevolgen voor de medewerkers van de ziekenhuizen. Zo kan er vermoeidheid optreden bij degenen die extra hard en lang moeten werken en/of wanneer er sprake is van stress als gevolg van de verhoogde werkdruk. De menselijke veerkracht die dat vereist, neemt daarbij sterk af naarmate de duur van de storing toeneemt. Voor de afdelingen waar ten gevolge van de ICT-uitval sprake was van overwerk en/of een crisissfeer, kan daarom aangenomen worden dat de prestaties afnamen terwijl de kans op fouten juist toenam. Ook hier geldt dat de duur van de ICT-uitval een belangrijke factor is bij het beheersbaar houden van de gevolgen voor de patiënt.

De afwegingen die dit van een afdeling vraagt in termen van veiligheid, worden geïllustreerd aan de hand van eerder genoemde situatie in het laboratorium van het Radboudumc. Daar moest aan het eind van de dag van de ICT-storing worden besloten welke medewerkers naar huis konden. De afweging was de achterstand zo snel mogelijk wegwerken, waarbij er door vermoeidheid een toenemende kans op het maken van menselijke fouten zou ontstaan, of het personeel zaterdagochtend verder laten werken waardoor medewerkers minder snel, maar wel uitgerust de achterstand zouden wegwerken. In verband met het weekend was er ruimte voor enige uitloop. Daarom werd besloten een aantal mensen naar huis te sturen zodat zij konden uitrusten, één persoon extra in te zetten in de nachtdienst en vijf extra mensen om 07:00 uur te laten beginnen. Op deze manier zou de afdeling ook over uitgerust personeel kunnen beschikken als de ICT-uitval zich zou voortzetten of herhalen. Zaterdag om 00:30 uur was het laboratorium bij met het analyseren en telefonisch rapporteren van de spoedeisende aanvragen. Op maandag waren ook de achterstanden op niet-spoedeisende zaken ingelopen en waren de handmatige invoer, openstaande analyses en afhandeling van resultaatopmerkingen gecontroleerd.

7. Medische apparatuur valt uit
De werking van medische apparatuur wordt steeds meer afhankelijk van ICT (zie ook hoofdstuk 2). Als het ICT-fundament uitvalt, kan ook de medische apparatuur uitvallen of overschakelen op de *stand alone* modus. In beide gevallen kan dit impact hebben op de patiëntveiligheid. Bij uitval van medische apparatuur kunnen diagnosevorming en monitoring van de toestand van de patiënt niet of slechts in beperkte mate plaatsvinden. Bij het overschakelen van apparatuur naar de *stand alone* modus kan geen automatische gegevensverwerking (verslaglegging) en integratie met de zorgsystemen (EPD) meer plaatsvinden. Dat kan ertoe leiden dat binnen de verschillende fasen van het zorgproces onvoldoende informatie voorhanden is om veilige en goede zorg te bieden.

In de onderzochte ziekenhuizen is, voor zover bekend op basis van bestudeerde documenten en interviews met betrokkenen, geen medische apparatuur uitgevallen. In de interviews wordt hierover bovendien aangegeven dat de medische apparatuur in de onderzochte ziekenhuizen ook in een *stand alone* modus kan draaien. Daarbij wordt in veel gevallen opgemerkt dat dit in de toekomst waarschijnlijk zal veranderen. Uitval van

medische apparatuur wordt door de Raad daarom beschouwd als een aandachtspunt voor ICT-ontwikkelingen binnen de ziekenhuizen (zie tevens hoofdstuk 2).

ICT-uitval kan op verschillende manieren gevolgen hebben voor de patiëntveiligheid. Voor zover bekend hebben de ICT-storingen in de onderzochte ziekenhuizen niet geleid tot letsel bij patiënten. Wel blijkt dat door de uitval van ICT in alle drie de onderzochte ziekenhuizen een verhoogde kans op schade aan patiënten is ontstaan.

4.2 Beperkte beeldvorming van gevolgen voor patiëntveiligheid

De crisisbeheersing in de onderzochte ziekenhuizen was erop gericht de gevolgen voor de patiënt en de patiëntveiligheid te minimaliseren. De onderzochte ziekenhuizen hebben na het optreden van de ICT-uitval mitigerende maatregelen genomen om te voorkomen dat er (een verhoogde kans op) schade aan patiënten zou ontstaan. Tijdens de voorvallen hadden de betrokkenen dan ook veel oog voor het waarborgen van de patiëntveiligheid. Dit heeft er volgens de onderzochte ziekenhuizen toe geleid dat de ICT-uitval niet of nauwelijks gevolgen heeft gehad voor de patiëntveiligheid. Gegeven de in de vorige paragraaf beschreven impact van ICT-uitval op de patiëntveiligheid, is dit een opvallende constatering. Hiervoor zijn drie oorzaken aan te wijzen.

4.2.1 Verhoogde kans op schade nauwelijks in beeld

Uit interviews met betrokkenen blijkt dat de vraag of de patiëntveiligheid tijdens de ICT-uitval in het geding is geweest, vooral beantwoord wordt in termen van daadwerkelijk opgetreden schade. Indien dergelijke schade zich niet heeft voorgedaan, is de patiëntveiligheid volgens hen niet in het geding geweest. Een verhoogde kans op schade, dat een belangrijk onderdeel is van patiëntveiligheid (zie paragraaf 1.6), blijft daarmee buiten beeld. Dit terwijl er door ICT-uitval op veel verschillende manieren een verhoogde kans op schade voor patiënten kan optreden. Zoals in paragraaf 4.1 is beschreven, kan het niet beschikbaar zijn van het EPD tot een beperkt beeld van de situatie van de patiënt leiden en tot onzekerheid over behandelmogelijkheden; kan een opnamestop tot langere aanrijdtijden leiden en tot minder adequate zorgmogelijkheden; beperkt het wegvallen van digitale communicatiesystemen de mogelijkheden om patiëntgegevens uit te wisselen en in noodsituaties alarm te slaan; verhoogt het werken met papieren dossiers het risico op zoekraken, verkeerd interpreteren en – na afloop van de ICT-uitval – foutief toevoegen van informatie; zet een terugval in efficiëntie het leveren van tijdige zorg onder druk; leidt vermoeidheid en/of stress tot het sneller maken van fouten; en beperkt de uitval van medische apparatuur de mogelijkheden voor diagnosevorming, monitoring en gegevensverwerking. Al deze gevolgen vergroten de kans op het ontstaan van schade.

4.2.2 Geen diepgaande analyse van gevolgen voor de patiëntveiligheid

De Raad constateert dat de beeldvorming van betrokkenen over de impact van het voorval op de patiëntveiligheid vooral gebaseerd is op *hear say* ('ik heb niet gehoord dat een patiënt schade heeft opgelopen als gevolg van de ICT-uitval'). Niet alle onderzochte ziekenhuizen zijn na de ICT-uitval op gestructureerde en diepgaande wijze nagegaan wat de impact van

het voorval was op de patiëntveiligheid. Ook in de evaluaties van de voorvallen zijn de gevolgen voor de patiëntveiligheid niet in alle gevallen inhoudelijk aan bod gekomen. Op basis hiervan constateert de Onderzoeksraad dat de gevolgen van de ICT-uitval voor de patiëntveiligheid na afloop van de storingen beperkt zijn geanalyseerd.

Voor een goed begrip van de gevolgen van de ICT-storingen is het nodig om op zorgvuldige wijze met alle betrokken zorgverleners het gesprek te voeren over de wijze waarop de (zorg)processen onder druk kwamen te staan en welke gevolgen dit had voor de patiëntveiligheid. Door hier geen aandacht aan te schenken, kan niet goed ingeschat worden op welke wijze ICT-uitval gevolgen kan hebben voor zorgverleners en patiënten en welke beheersmaatregelen genomen moeten worden om de gevolgen voor de patiëntveiligheid van soortgelijke voorvallen in de toekomst te voorkomen.

4.2.3 Schade aan uitgeweken patiënten buiten beeld

Uit interviews met betrokkenen bij de voorvallen blijkt dat de vraag of de patiëntveiligheid tijdens de ICT-uitval in het geding is geweest, hoofdzakelijk wordt beantwoord met betrekking tot patiënten die bij het ziekenhuis onder behandeling zijn. De patiënten die door de ICT-uitval naar een ander ziekenhuis moesten uitwijken, blijven hierbij buiten beeld. Terwijl er in die gevallen wel degelijk (een verhoogde kans op) schade kan optreden, bijvoorbeeld door een langere reistijd, het ontbreken van expertise elders, langere wachttijden en/of een gebrek aan informatie over de patiënt (zie paragraaf 4.1). Dat ziekenhuizen zich richten op eigen patiënten is in lijn met de wettelijke taak van ziekenhuizen. Zij zijn verantwoordelijk voor de kwaliteit van de geleverde zorg aan patiënten die bij hen onder behandeling zijn. De Nederlandse Zorgautoriteit en de zorgverzekeraars zijn verantwoordelijk voor voldoende opnamecapaciteit in de regio. Deze taakverdeling zorgt ervoor dat de onderzochte ziekenhuizen – naast het mogelijk ontvangen van TIM-meldingen[84] van collega-ziekenhuizen, de meldkamer en/of de medisch manager ambulance – na afloop van het incident niet zelf actief zijn nagegaan of patiënten die moesten uitwijken naar andere ziekenhuizen schade hebben opgelopen. Er is ook geen andere partij in het veld die dit wel in kaart heeft gebracht. Het beeld over de eventuele gevolgen van ICT-uitval voor de patiëntveiligheid is daarmee onvolledig.

Na afloop van de voorvallen hebben de ziekenhuizen zich een beperkt beeld gevormd van de gevolgen voor de patiëntveiligheid. De bij de voorvallen opgetreden verhoogde kans op schade voor patiënten bleef grotendeels buiten beschouwing, er werd met weinig diepgang gekeken naar de gevolgen van de ICT-uitval voor de veiligheid van de patiënten in het ziekenhuis en de veiligheid van (door de ICT-storing) omgeleide patiënten bleef buiten beeld.

84 TIM staat voor Transmuraal Incidenten Melden. Dit is een vergelijkbaar systeem als VIM, maar dan gericht op de ketenzorg.

4.3 Conclusie

Uit het onderzoek blijkt dat de risico's voor de patiëntveiligheid bij ICT-uitval reëel zijn. De Onderzoeksraad constateert dat de onderzochte ziekenhuizen tijdens het incident veel aandacht hadden voor de patiëntveiligheid, maar ook dat ze zich *na afloop* een beperkt beeld hebben gevormd van de gevolgen van de ICT-uitval voor de patiëntveiligheid. Zo baseren de ziekenhuizen hun antwoord op de vraag of de patiëntveiligheid tijdens de ICT-uitval in het geding is geweest hoofdzakelijk op daadwerkelijk opgetreden schade en niet of nauwelijks op het ontstaan van onveilige situaties voor de patiënt. Hierdoor blijft een belangrijk aspect van patiëntveiligheid, namelijk een verhoogde kans op schade aan de patiënt, grotendeels buiten hun blikveld. Daar komt bij dat met weinig diepgang is gekeken naar de gevolgen van de ICT-uitval voor de veiligheid van de patiënten in het ziekenhuis en dat noch de ziekenhuizen noch andere partijen in het veld zicht hebben op de (verhoogde kans op) schade die eventueel is ontstaan doordat patiënten naar een ander ziekenhuis moesten uitwijken. Het beperkte zicht op de gevolgen van ICT-uitval voor de patiëntveiligheid beperkt ziekenhuizen om van voorvallen te leren.

5 AANKNOPINGSPUNTEN RISICOBEHEERSING ICT-UITVAL

In hoofdstuk 3 stonden de ICT-storingen centraal die zich hebben voorgedaan in het Radboudumc, het IJsselland Ziekenhuis en Dijklander Ziekenhuis. Daarbij zijn zowel de directe oorzaken van de voorvallen geïdentificeerd, als voorvaloverstijgende factoren. Deze factoren hebben zich voorgedaan op operationeel niveau en geven op dat niveau inzicht in de manier waarop de kans op ICT-uitval verkleind en de gevolgen van ICT-uitval voor de patiëntveiligheid beperkt kunnen worden. In hoofdstuk 4 is vervolgens de vraag beantwoord wat de gevolgen van de ICT-uitval voor de patiëntveiligheid kunnen zijn. In dit hoofdstuk worden vanuit de organisatorische context waarbinnen de onderzochte voorvallen plaatsvonden, aanknopingspunten geïdentificeerd om de risico's op ICT-uitval in ziekenhuizen en de gevolgen hiervan voor de patiëntveiligheid vroegtijdig in beeld te krijgen en adequaat te beheersen.

5.1 Organisatiebreed risicobesef

De Onderzoeksraad ziet een gedeeld risicobesef binnen ziekenhuizen als belangrijke voorwaarde om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid op adequate wijze te beheersen. Daarbij is het van belang dat het risicobesef zich niet beperkt tot enkele individuen of tussen zorgafdelingen aan de ene kant en de ICT-afdeling aan de andere kant, maar binnen de organisatie gedeeld wordt. Pas dan kan adequate risicobeheersing daadwerkelijk van de grond komen.

In alle drie de onderzochte ziekenhuizen is ICT-uitval in de crisisplannen benoemd als belangrijk risico. Uit het onderzoek van de Raad blijkt dat deze risico-inschatting in beperkte mate bredere weerslag vindt binnen de ziekenhuisorganisaties. Op verschillende niveaus binnen de organisaties schatten sommige medewerkers het risico als hoog in, anderen beoordelen ICT-uitval als een beperkt risico. Door het ontbreken van een gedeeld risicobesef worden de risico's beperkt vertaald in te nemen beheersmaatregelen. Zo was bij geen van de drie ziekenhuizen naar aanleiding van de hoge risicoschatting in de crisisplannen een concrete uitwerking beschikbaar om de crissisorganisatie voor te bereiden op het daadwerkelijk optreden van ICT-uitval. Ook wordt een dergelijk scenario niet of uitsluitend op beperkte schaal op realistische wijze geoefend en worden ICT-systemen nauwelijks in samenhang met andere systemen getest.

Uit het onderzoek komt naar voren dat onvoldoende op ieders netvlies staat hoe en welke onveilige situaties door uitval van ICT kunnen ontstaan. Daar komt bij dat er vanuit de evaluaties van de voorvallen het beeld is ontstaan dat de ICT-uitval niet of nauwelijks gevolgen heeft gehad voor de patiëntveiligheid, terwijl uit voorliggend onderzoek blijkt dat er wel degelijk sprake was van een verhoogde kans op schade voor patiënten (zie hoofdstuk 4).

Een goed risicobesef is ook van belang voor andere partijen in het veld. De Onderzoeksraad constateert dat de ziekenhuiszorg in toenemende mate kwetsbaar is voor ICT-uitval in meerdere ziekenhuizen tegelijk, zie hiervoor ook figuur 4 in paragraaf 1.1. Als gevolg hiervan kan de regionale opvangcapaciteit van ziekenhuizen onder druk komen te staan. Deze kwetsbaarheid kwam bijvoorbeeld in 2017 in Groot-Brittannië naar voren, toen meerdere ziekenhuizen in (de omgeving van) Londen tegelijk geraakt werden door de WannaCry ransomware aanval.[85] In Nederland speelde regiocapaciteit onder meer een rol bij de ICT-storing in de Noordwest Ziekenhuisgroep in januari 2019, waarbij meerdere locaties van de groep werden getroffen door een storing. In verband met de daar opgetreden ICT-uitval werden poli's gesloten, OK-programma's geschrapt, en werd een opnamestop voor de SEH afgekondigd. Ambulances werd gevraagd geen patiënten meer naar de locaties in Alkmaar en Den Helder te brengen. Omdat de reistijd voor patiënten die omgeleid moesten worden daarmee te lang zou kunnen worden, werd echter tevens besloten om instabiele patiënten en patiënten die gereanimeerd moesten worden wel toe te laten tot de SEH. Ook bij veel andere ICT-storingen in ziekenhuizen werden meerdere locaties getroffen. Dit laat zien dat grootschalige en ziekenhuis-overstijgende ICT-uitval, een serieus risico vormt voor de veiligheid van de patiënt.

Aan de basis van adequate risicobeheersing ligt een gedeeld besef dat (zorg) processen in toenemende mate afhankelijk zijn van ICT en dat ICT-uitval risico's met zich meebrengt voor de veiligheid van patiënten. Aandacht en uitwerking van deze risico's in alle lagen van de ziekenhuisorganisatie is een belangrijke stap richting adequate beheersing van de risico's van ICT-uitval voor patiënten.

5.2 Prioritering ten opzichte van andere risico's en ontwikkelingen

Om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid te kunnen beheersen, is bestuurlijke aandacht onontbeerlijk. Het risico op uitval van ICT heeft in de bestuurskamer van een ziekenhuis echter veel concurrentie van andere risico's en ontwikkelingen. Ziekenhuisbestuurders worden geconfronteerd met diverse onderwerpen en ontwikkelingen, zoals schaalvergroting (fusies), lateralisatie (verplaatsen van zorg naar een andere locatie), extramuralisering, netwerksamenwerking en de noodzaak tot beheersing van zorguitgaven. Deze ontwikkelingen vragen veel tijd en aandacht, wat ten koste kan gaan van aandacht voor het voorkomen en beheersen van ICT-uitval.

Als het gaat om de patiëntveiligheid krijgen vooral risico's die direct gerelateerd zijn aan de patiëntenzorg de aandacht van ziekenhuizen. Hierbij kan bijvoorbeeld gedacht worden aan het risico van wondinfecties na een operatie of aan de risico's die samenhangen met onvoldoende handhygiëne. Deze risico's staan traditioneel hoog op de prioriteitenlijst van ziekenhuizen. In het Programma VMS 2008 – 2012, aan de hand waarvan alle ziekenhuizen in Nederland een geaccrediteerd of gecertificeerd

85 National Audit Office. "Investigation: WannaCry cyber-attack and the NHS. HC 414 SESSION 2017–2019", 25 april 2018.

veiligheidsmanagementsysteem (VMS) implementeren, werd bijvoorbeeld met name aan dit soort direct aan patiëntenzorg gerelateerde thema's gewerkt.[86] Ook op de afdelingen Kwaliteit en Veiligheid binnen de onderzochte ziekenhuizen wordt vooral naar deze 'zorgthema's' gekeken.[87] Het omgaan met ICT-gerelateerde risico's zou daar, gelet op de toegenomen afhankelijkheid van ICT, aan toegevoegd moeten worden.

Met betrekking tot ICT-gerelateerde risico's hebben ziekenhuizen vooral aandacht voor risico's rondom gegevensuitwisseling, cybercrime en datalekken. Ook sectorbreed leven met name deze onderwerpen. Zo heeft de sector een aantal jaar geleden een expertisecentrum op het gebied van cybersecurity in de zorg (Z-CERT) opgericht[88], dat zich vooral richt op cybercrime. Voor niet-intentionele ICT-storingen is geen aandacht. Dit geldt ook voor de relevante overheidspartijen. Zo is het ministerie van VWS een aanjager van digitalisering in de zorg, waarbij vooral ingezet wordt op intensiveringsmiddelen voor innovatieve werkwijzen, het vergroten van digitale en innovatieve vaardigheden[89] en velerlei acties gericht op implementatie en opschaling.[90] Ook in de programma's en hoofdlijnenakkoorden hebben onderwerpen als innovatieve zorg en e-health een belangrijke plek.[91] De aandacht die er is voor risico's, is vooral gericht op informatie-uitwisseling in de zorg. Om de problemen daarmee, en de risico's hiervan voor de patiëntveiligheid het hoofd te bieden, heeft de minister voor Medische Zorg en Sport aangekondigd om zorgverleners en zorginstellingen te verplichten tot digitale dossiervoering en tot elektronische gegevensuitwisseling.[92] Ook cybercrime en datalekken krijgen aandacht van de minister. Zo heeft het ministerie het opzetten van het eerder genoemde Z-CERT ondersteund en is in samenwerking met brancheorganisaties het *Actieplan Informatiebeveiliging in de medisch-specialistische zorg en geestelijke gezondheidszorg* opgesteld.[93] Soortgelijke beleidsinitiatieven ontbreken voor het risico op (niet-intentionele) ICT-storingen in ziekenhuizen en de gevolgen hiervan voor de patiëntveiligheid.

Ziekenhuisbestuurders kunnen door toezichthoudende instanties en accrediterende organisaties geprikkeld worden om aandacht te besteden aan bepaalde onderwerpen. Een belangrijke toezichthoudende instantie voor ziekenhuizen is de IGJ. De IGJ kijkt sinds het najaar van 2017 naar de inzet van ICT door ziekenhuizen. Dit doet ze met behulp van het toetsingskader "*Inzet van e-health door zorgaanbieders*". Dit toetsingskader is

86 www.vmszorg.nl.
87 Elk ziekenhuis kent één of meerdere afdelingen die betrokken zijn bij het sturen op de kwaliteit en veiligheid van de zorg. De benamingen van deze afdelingen kunnen per ziekenhuis verschillen. In dit rapport wordt gesproken over de afdeling Kwaliteit en Veiligheid.
88 De initiatiefnemers hiervan waren de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en GGZ Nederland (GGZ).
89 Een voorbeeld hiervan is het communicatietraject "*Zorg van Nu*", met het doel om het algemene publiek en professionals te wijzen op de kansen en mogelijkheden van innovaties in de zorg en in nieuwe zorgprocessen. Bron: Ministerie van VWS, 2018, *Voortgangsrapportage eHealth en zorgvernieuwing*, 18 mei 2018.
90 Bijvoorbeeld de VIPP-programma's in de medisch specialistische zorg (in uitvoering) en de GGZ (in ontwikkeling) en het eerstelijnsprogramma OPEN (in ontwikkeling) waarmee gegevensuitwisseling vereenvoudigd wordt en instellingen en huisartsen gestimuleerd worden medische gegevens van patiënten digitaal beschikbaar te stellen aan patiënten, zodat zij ook thuis hun eigen gegevens kunnen inzien. Bron: Minister van VWS, *Voortgangsrapportage eHealth en zorgvernieuwing*, 18 mei 2018.
91 Ministerie van VWS (2018), *Voortgangsrapportage eHealth en zorgvernieuwing*, 18 mei 2018.
92 Ministerie van VWS (2019). Tweede Kamer, vergaderjaar 2018–2019, 27 529, nr. 183.
93 Actieplan *Informatiebeveiliging in de medisch-specialistische zorg en geestelijke gezondheidszorg,* Z-Cert, 14 juni 2017.

gericht op het creëren van de juiste randvoorwaarden voor de inzet van *e-health* door zorgaanbieders, waarbij de daarmee samenhangende risico's zo goed mogelijk beheerst dienen te worden. Een ander instrument van de IGJ is het convenant "*Veilige toepassing van medische technologie in de medisch specialistische zorg*", dat gericht is op de risicobeheersing en veilige toepassing van medische technologie[94] binnen de zorg. De inspectie treedt vanaf 1 januari 2016 handhavend op met betrekking tot de implementatie van het convenant door ziekenhuizen, omdat ze het convenant als een belangrijke voorwaarde voor verantwoorde zorg ziet.[95] Hiermee heeft de IGJ twee instrumenten in handen die ziekenhuizen ertoe zouden kunnen aansporen het risico op ICT-uitval beter te beheersen. Bij beide instrumenten vormt de inrichting en het beheer van het ICT-fundament geen afzonderlijk thema.

Tot slot toetsen de belangrijkste accrediterende instanties voor ziekenhuizen, het NIAZ[96] en de JCI[97], tot op heden in beperkte mate op de beheersing op en van risico's van ICT-uitval en de gevolgen hiervan voor een verhoogde kans op schade aan patiënten. Wel signaleert de Onderzoeksraad dat de JCI in toenemende mate aandacht voor dit onderwerp heeft.

Om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid beter te kunnen beheersen, dient het in de bestuurskamer een hoge prioriteit te krijgen. Het ministerie van VWS, de IGJ en de accrediterende instanties voor ziekenhuizen kunnen hieraan bijdragen door vanuit hun eigen rol de aandacht voor (het beheersen van) de risico's van ICT-uitval voor de patiëntveiligheid te vergroten.

5.3 Veerkracht én voorbereiding

Uit het onderzoek van de Raad blijkt dat voor het beheersen van de gevolgen van uitval van ICT binnen ziekenhuizen, vooral wordt vertrouwd op de veerkracht van het medisch personeel.[98] In interviews gaven betrokkenen veelvuldig aan dat medisch personeel gewend is om te improviseren en in onvoorspelbare situaties te opereren. De veerkracht van het medisch personeel werd daarmee gezien als een belangrijke beheersmaatregel.

94 Medische technologie is de toepassing van georganiseerde kennis en vaardigheden in de vorm van apparaten, medicijnen, vaccins, procedures en systemen, die ontwikkeld zijn om gezondheidsproblemen op te lossen en de kwaliteit van leven te verbeteren.

95 IGJ, "*Toezicht op implementatie Convenant Medische Technologie*", 2015.

96 Het Nederlands Instituut voor Accreditatie in de Zorg (NIAZ) ontwikkelt kwaliteitsnormen en toetst zorginstellingen hierop. Beoordeeld wordt of zorginstellingen hun organisatie zo hebben ingericht dat zij op een reproduceerbare wijze een acceptabel kwaliteitsniveau van zorg voortbrengen. Als dat het geval is, krijgt de instelling een accreditatie voor vier jaar. Deelname aan het programma van het NIAZ is vrijwillig en geschiedt altijd op verzoek van de zorginstelling zelf. De toetsing vindt plaats op basis van tevoren bekende en gepubliceerde normen en een overeenkomstige auditprocedure.

97 JCI-accreditatie is een internationaal keurmerk voor ziekenhuizen. De missie van JCI is het verbeteren van de veiligheid en kwaliteit van zorg.

98 Met veerkracht wordt hier bedoeld het handelend optreden tijdens een crisis en niet de vaardigheid om na een crisis en/of stressvolle situatie weer snel "normaal" te kunnen functioneren.

Een goede beheersing van de gevolgen van ICT-uitval voor de patiëntveiligheid is, in aanvulling op de veerkracht van het personeel, echter in belangrijke mate afhankelijk van een goede voorbereiding. Medisch personeel kan namelijk in steeds mindere mate terugvallen op analoge alternatieven, doordat deze worden uitgefaseerd en/of doordat de kennis en vaardigheden om hiermee te werken zullen teruglopen.

Om de risico's op en van ICT-uitval te beheersen, verwacht de Onderzoeksraad dat ziekenhuisbesturen medewerkers vanwege de toenemende digitalisering van de zorg voorbereiden om hun rol tijdens een crisis optimaal te kunnen vervullen. Daarvoor is het nodig dat ziekenhuisbesturen de ICT-afhankelijkheden in zorgprocessen in kaart brengen en de gevolgen doordenken die ICT-uitval kan hebben voor de patiëntveiligheid. Ook dient er kritische aandacht te zijn voor het opleiden en trainen van personeel en het oefenen met ICT-uitvalscenario's.

Op grond van hun verantwoordelijkheid voor kwaliteit van zorg, kunnen ziekenhuizen niet alleen vertrouwen op de veerkracht van het (medisch) personeel. Veerkracht dient aangevuld te worden met een gedegen voorbereiding van de ziekenhuisorganisatie op het beheersen van de gevolgen bij een eventuele grootschalige ICT-uitval.

5.4 Bij elkaar brengen van zorg en ICT

Om de risico's van ICT-uitval te beheersen, is het naar mening van de Onderzoeksraad van belang dat "de zorg" en "de ICT" elkaar vinden. Door een brug te slaan tussen beide werelden kunnen ICT-afhankelijkheden binnen zorgprocessen en de risico's hiervan voor de patiëntveiligheid bij ICT-uitval, in kaart worden gebracht.

Uit het onderzoek van de Raad naar de drie voorvallen komt naar voren dat de onderzochte ziekenhuizen stappen zetten in het dichter bij elkaar brengen van de zorgwereld en de ICT-wereld. Een belangrijke ontwikkeling hierbij is het aanstellen van een *Chief Medical Information Officer* (CMIO) en een *Chief Nurse Information Officer* (CNIO). Dit zijn artsen en verpleegkundigen die de verbinding vormen tussen de patiëntenzorg en de ICT. De Raad constateert dat deze verbinding vooral nog gelegd wordt bij de opzet en uitvoering van ICT-gerelateerde project- en programmavoorstellen en bij het vertalen van behoeften uit de zorgpraktijk naar ICT-oplossingen. De aandacht gaat daarbij voornamelijk uit naar ICT-innovatie en project- en programma-gerelateerde ICT-risico's. De risico's van ICT-uitval voor de patiëntveiligheid, waaronder nieuwe risico's die kunnen voortkomen uit de voortgaande digitalisering in de zorg, blijven grotendeels buiten beeld. Daarbij speelt ook dat de functies van CMIO en CNIO niet in alle ziekenhuizen fulltime zijn, waardoor er beperkt tijd is om de functie uit te oefenen en tijd vrij te maken voor de inventarisatie en beheersing van ICT-risico's.

Afdelingen Kwaliteit en Veiligheid, die belast zijn met de implementatie van het VMS, kunnen ook bijdragen aan het verder bij elkaar brengen van "de zorg" en "de ICT". Hoewel deze afdelingen zich traditioneel op zorgthema's richten, leidt de toenemende aandacht voor het convenant "*Veilige toepassing van medische technologie in de medisch specialistische zorg*" ertoe dat ook ICT-toepassingen in hun aandachtsgebied komen. Dit zorgt er (onder meer) voor dat bij invoering van nieuwe medische technologie, waaronder grootschalige softwaretoepassingen als het EPD, risico's systematisch in kaart worden gebracht aan de hand van een multidisciplinaire Prospectieve Risico Inventarisatie[99]. Bij kleinere software-aanpassingen is dit echter niet vanzelfsprekend en ook wijzigingen aan het ICT-fundament komen niet of slechts in beperkte mate aan bod. De risico's die hiermee samenhangen worden vooral gezien als een verantwoordelijkheid voor de ICT-afdeling. Bij de risicobeheersing vanuit de ICT ontbreekt het echter vaak aan een doorvertaling naar beheersmaatregelen die gericht zijn op het waarborgen van de kwaliteit en veiligheid van de patiëntenzorg. Het resultaat is dat met betrekking tot het risico op ICT-uitval, er geen gezamenlijke doorlichting van de zorgprocessen plaatsvindt. Daardoor worden ICT-afhankelijkheden niet geïdentificeerd en worden er in onvoldoende mate beheersmaatregelen getroffen om de beschikbaarheid van systemen voor het zorgproces te waarborgen en/of de uitval van ICT op andere wijzen te kunnen ondervangen.

Ook bij een ander element van het VMS, het leren van incidenten op basis van VIM-meldingen, ligt de focus vooral op de zorg en is er weinig aandacht voor de rol van ICT. Dit komt doordat bij de analyse van VIM-meldingen niet altijd gekeken wordt naar de diepere, achterliggende oorzaken. Bovendien wordt bij het bespreken en analyseren van incidentmeldingen wel medisch personeel betrokken, maar is de betrokkenheid van ICT-personeel organisatorisch niet in alle gevallen structureel en/of in voldoende mate ingebed. Dit zorgt ervoor dat als ICT op de achtergrond een rol speelt bij een veiligheidsincident, dit niet in alle gevallen in beeld komt. ICT-afhankelijkheden binnen het zorgproces, en daarmee de risico's van ICT-uitval voor de patiëntveiligheid, komen daardoor niet altijd in zicht. Dat belemmert eveneens het nemen van passende maatregelen om de achterliggende oorza(a)k(en) weg te nemen.

Tot slot kan ook bij de crisisorganisatie de verbinding tussen "de zorg" en "de ICT" verbeterd worden. Zo kunnen er meer initiatieven ontplooid worden om zich gezamenlijk voor te bereiden op het optreden van een ICT-crisis, zoals uitval van ICT. Daardoor kan bewerkstelligd worden dat bij een voorval snel duidelijk is welke zorgprocessen onder druk komen te staan door de uitval van ICT. Ook dienen voor een optimale samenwerking tijdens de bestrijding van de crisis de opschalingsprocedures tussen de ICT-afdeling en daaraan verbonden externe partijen enerzijds, en de crisisorganisatie anderzijds, goed op elkaar aan te sluiten. Betere afstemming en samenwerking tussen de zorg en ICT kan daarmee bijdragen aan een adequate beheersing van de risico's op en van ICT-uitval voor de patiëntveiligheid.

99 Een Prospectieve Risico Inventarisatie is een middel om voor risicovolle processen de risico's gestructureerd inzichtelijk te maken en voor de grootste risico's zoveel mogelijk mitigerende maatregelen te nemen.

Voor een adequate beheersing van het risico op en van ICT-uitval is het nodig de werelden van “de zorg” en “de ICT” bij elkaar te brengen en de samenwerking tussen beiden op gestructureerde wijze in te bedden in de ziekenhuisorganisatie. Daarbij dient niet alleen aandacht te zijn voor de kansen van ICT, maar ook voor het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid.

5.5 Conclusie

De analyse van de organisatorische context waarin de drie onderzochte voorvallen plaatsvonden, biedt aanknopingspunten om het risico op ICT-uitval en de gevolgen hiervan voor de patiëntveiligheid op adequate wijze te beheersen. Het is hiervoor van belang dat raden van bestuur hier de juiste prioriteit aan geven en werken aan een gedeeld risicobesef onder medewerkers met betrekking tot ICT-uitval en de gevolgen daarvan voor de patiëntveiligheid. In aanvulling op het vertrouwen op veerkracht van het personeel vraagt dit om een gedegen voorbereiding op ICT-uitval. Het is ten slotte van belang om zorg en ICT in alle lagen van de organisatie bij elkaar te brengen en de samenwerking hiertussen te borgen in de organisatie.

6 CONCLUSIES

De Onderzoeksraad voor Veiligheid heeft zich in dit onderzoek gericht op de vraag hoe ziekenhuizen de risico's van ICT-storingen voor de patiëntveiligheid op adequate wijze kunnen beheersen. Hij heeft daartoe drie ICT-storingen in ziekenhuizen onderzocht en drie ICT-storingen beschouwd. Dit onderzoek leidt tot de onderstaande hoofdconclusie.

Digitalisering is doorgedrongen tot het hart van de zorg. Nagenoeg alle processen in het ziekenhuis zijn inmiddels (in meer of mindere mate) gedigitaliseerd. Daardoor is adequate diagnosestelling en behandeling zonder digitale technieken nauwelijks meer mogelijk. Dit heeft ertoe geleid dat ziekenhuizen voor het leveren van goede en veilige zorg sterk afhankelijk zijn van het goed functioneren van ICT. Grootschalige ICT-uitval kan daardoor direct gevolgen hebben voor de patiëntveiligheid. De Onderzoeksraad constateert dat de bewustwording van het risico op en van ICT-uitval in ziekenhuizen niet in gelijke mate is meegegroeid met de toegenomen afhankelijkheid van ICT. Om de risico's voor patiënten beter te beheersen, is meer aandacht nodig voor het voorkomen en bestrijden van ICT-uitval en voor de gevolgen van ICT-uitval voor de veiligheid van patiënten.

De bovenstaande hoofdconclusie is gebaseerd op onderstaande vier deelconclusies.

1. ICT-afhankelijkheid binnen zorgprocessen
De (medisch-specialistische) zorgverlening in ziekenhuizen is door de digitalisering dermate afhankelijk geworden van ICT, dat grootschalige ICT-uitval kan leiden tot onveilige situaties voor patiënten. Voor een goede en veilige behandeling van patiënten is het van belang dat ziekenhuizen de afhankelijkheden van ICT binnen (zorg)processen in kaart brengen.

2. Voorkomen, bestrijden en beheersen gevolgen ICT-uitval
Het voorkomen van ICT-uitval vereist een goede inrichting en beheer van het ICT-fundament. Het voorkomen van uitval van ICT, het vermogen om storingen zo snel mogelijk te kunnen verhelpen als deze zich toch voordoen en het beheersen van de gevolgen ervan vraagt daarnaast om een goede voorbereiding en het adequaat leren van ICT-voorvallen. Onvolkomenheden in de gemaakte keuzes bij de inrichting en het beheer van het ICT-fundament, alsmede bij de voorbereiding op ICT-uitval, hebben bijgedragen aan het langdurig uitvallen van de ICT bij de door de Raad onderzochte voorvallen.

3. Gevolgen van ICT-uitval voor de patiëntveiligheid

De Onderzoeksraad onderscheidt zeven manieren waarop ICT-uitval tot (een verhoogde kans op) schade aan patiënten kan leiden. Voor het leren van voorvallen en een adequate beheersing van de risico's van ICT-uitval, is het van belang dat ziekenhuizen hier een goed zicht op hebben. Tijdens de ICT-storingen stond patiëntveiligheid in de afwegingen van professionals en managers steeds voorop. Na *afloop* van de storingen is niet of nauwelijks systematisch nagegaan wat de gevolgen ervan zijn geweest. Zo baseren de ziekenhuizen hun antwoord op de vraag of de patiëntveiligheid tijdens de ICT-uitval in het geding is geweest hoofdzakelijk op daadwerkelijk opgetreden schade en niet of nauwelijks op het ontstaan van onveilige situaties voor de patiënt. Ook is er na afloop van de incidenten over het algemeen niet of met weinig diepgang gekeken naar de gevolgen van de ICT-uitval voor de patiëntveiligheid. Tenslotte hebben de onderzochte ziekenhuizen noch andere partijen in het veld een beeld van de eventuele schade die is ontstaan doordat patiënten naar een ander ziekenhuis moesten uitwijken.

4. Noodzaak van bestuurlijke aandacht voor ICT-uitval

Bestuurlijke aandacht voor de risico's van ICT-uitval en de gevolgen daarvan voor de patiëntveiligheid is onontbeerlijk voor een adequate beheersing van die risico's. Daarbij zouden vooral de punten uit de voorgaande drie deelconclusies aandacht moeten krijgen. Ook is een gedeeld risicobesef onder medewerkers van belang en zouden de werelden van zorg en ICT nader bij elkaar gebracht moeten worden met het oog op het tijdig onderkennen van de risico's op ICT-uitval en de mogelijke gevolgen daarvan voor goede en veilige zorg.

7 AANBEVELINGEN

Ziekenhuizen zijn voor het leveren van goede zorg steeds meer afhankelijk van het goed functioneren van ICT. Uit dit onderzoek blijkt dat ICT-uitval de patiëntveiligheid in het geding kan brengen. De Raad ziet op basis van zijn onderzoek aanknopingspunten om de risico's op ICT-uitval in ziekenhuizen en de gevolgen hiervan voor de patiëntveiligheid vroegtijdig in beeld te krijgen en adequaat te beheersen. Enerzijds door beter te sturen op het voorkomen van uitval van ICT, anderzijds door de organisatie beter voor te bereiden op het beheersen van de gevolgen van uitval van ICT.

De frequentie en duur van ICT-storingen in ziekenhuizen laten zien dat er sprake is van een vraagstuk dat breder speelt. De Raad kiest er daarom voor zich in zijn aanbevelingen niet te beperken tot de drie onderzochte ziekenhuizen, maar zich tot alle ziekenhuizen in Nederland te richten. Om te bevorderen dat ziekenhuizen het vraagstuk gezamenlijk benaderen en van en met elkaar leren om de ICT-risico's beter te beheersen, doet de Onderzoeksraad aanbevelingen aan de twee grootste brancheverenigingen. De Raad ziet ook een rol weggelegd voor de IGJ.

Aan de Nederlandse Vereniging van Ziekenhuizen (NVZ) en de Nederlandse Federatie van Universitair Medische Centra (NFU):

1. Bewerkstellig dat uw leden:

    a. Met het oog op een goede voorbereiding op uitval van ICT, de afhankelijkheden tussen zorg en ICT periodiek in kaart brengen, inclusief de mogelijke risico's voor patiënten die gepaard gaan met ICT-uitval.
    b. Periodiek de ICT-systemen in samenhang testen, om te borgen dat de kritische zorgprocessen onder alle omstandigheden blijven functioneren. Ook dient geoefend te worden met scenario's waarbij de ICT in het ziekenhuis uitvalt. Betrek daar waar zinvol de leveranciers bij deze oefeningen en testen.
    c. Na elke ernstige ICT-uitval evaluaties uitvoeren waarbij ook de (verhoogde kans op) schade voor zowel de patiënten in het ziekenhuis als voor de uitgeweken patiënten diepgaand wordt geanalyseerd. Betrek daarbij waar nodig de partners in de zorgketen.
    d. Over alle drie de hierboven genoemde aspecten jaarlijks publiek verantwoording afleggen.

2. Borg dat ziekenhuizen dit vraagstuk gezamenlijk benaderen en van en met elkaar leren.

Lees verder op de volgende pagina

3. Ontwikkel een praktisch handvat voor ziekenhuizen voor het beheersen van de risico's van uitval van ICT, waarin de in dit rapport genoemde aanknopingspunten worden meegenomen.

4. Ga in regionaal verband na of in geval van ICT-uitval waarbij meerdere ziekenhuislocaties in een regio worden getroffen, de veiligheid van patiënten voldoende is geborgd.

Aan de Inspectie Gezondheidszorg en Jeugd (IGJ):

5. Besteed in het toezicht op ziekenhuizen aandacht aan de punten in bovengenoemde aanbevelingen.

BIJLAGE A

ONDERZOEKSVERANTWOORDING

Aanleiding voor het onderzoek

Door de digitalisering van de zorg zijn ziekenhuizen in toenemende mate afhankelijk van ICT voor het leveren van goede en veilige zorg. De Onderzoeksraad vraagt zich gegeven deze ontwikkeling af in hoeverre ICT-uitval de veiligheid van patiënten in gevaar kan brengen. Daarom heeft de Raad een onderzoek ingesteld naar de ICT-storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis, in relatie tot de patiëntveiligheid. Deze incidenten zijn geselecteerd naar type en grootte van het ziekenhuis, het moment waarop de storing zich heeft voorgedaan (kort voor of tijdens het lopende onderzoek), de duur en de omvang van de storing.

Doelstelling

De Onderzoeksraad wil met dit rapport een bijdrage leveren aan de (verdere) verbetering van de patiëntveiligheid in Nederlandse ziekenhuizen. Hij doet dat door lessen te trekken uit bovengenoemde drie ICT-storingen om ziekenhuizen in Nederland beter in staat te stellen om i) ICT-storingen te voorkomen en te bestrijden; en ii) de veiligheidsrisico's voor patiënten als gevolg van ICT-storingen te kunnen beheersen. Het is nadrukkelijk niet het doel van het onderzoek om een oordeel te vellen over de drie onderzochte ziekenhuizen noch om lessen te formuleren die alleen op hen betrekking hebben. De drie voorvallen zijn benut als cases om zicht te krijgen op het algemene vraagstuk van patiëntveiligheid in relatie tot ICT-uitval. De Raad streeft ernaar lessen te trekken op een dusdanig niveau, dat deze van nut zijn voor alle ziekenhuizen.

Onderzoeksvragen

De volgende hoofdvraag staat centraal in dit onderzoek:

> Hoe kunnen ziekenhuizen de risico's van ICT-storingen voor de patiëntveiligheid op adequate wijze beheersen?

De hoofdvraag valt uiteen in de volgende deelvragen:

a. Hoe zijn de ICT-storingen ontstaan, bestreden en de gevolgen ervan beheerst?
b. Welke risico's brengen ICT-storingen met zich mee voor patiëntveiligheid?
c. Hoe worden de risico's van ICT-storingen voor patiëntveiligheid binnen de onderzochte ziekenhuizen beheerst?
d. Welke organisatiefactoren binnen de onderzochte ziekenhuizen belemmeren een adequate beheersing van de risico's van ICT-uitval voor de patiëntveiligheid?

e. Hoe kan het systeem voor een adequate beheersing van de risico's van ICT-uitval voor de patiëntveiligheid worden verbeterd?

Afbakening

Dit onderzoek richt zich op ziekenhuisorganisaties, omdat zij verantwoordelijk zijn voor de kwaliteit van zorg. Zorginstellingen kunnen echter niet los worden gezien van het systeem waar zij onderdeel van uitmaken. Daarom komt soms ook de rol van andere partijen ter sprake, zoals het Ministerie van VWS en de Inspectie voor IGJ.

Bij het begrip informatieveiligheid wordt doorgaans onderscheid gemaakt tussen beschikbaarheid, integriteit en vertrouwelijkheid.[100] Dit onderzoek beperkt zich tot de beschikbaarheid. Daarmee vallen onderwerpen als datalekken en het vertrouwelijk omgaan met informatie buiten de scope van het onderzoek. Hoewel integriteit van data geen onderdeel uitmaakt van dit onderzoek, hebben maatregelen die hierop genomen worden wel invloed op de patiëntveiligheid. Dit is bijvoorbeeld aan de orde wanneer ziekenhuizen na een ICT-storing patiëntendossiers moeten actualiseren en controleren. De integriteit van data komt daarom zijdelings aan bod in dit onderzoek.

Waar in dit onderzoek wordt gesproken over ziekenhuizen, gaat het over de instellingen voor medisch specialistische zorg, die zowel klinische als poliklinische zorg verlenen. Dit betreft de algemene ziekenhuizen[101], de universitair medische centra en de categorale instellingen.

ICT-uitval kan veroorzaakt worden door intentioneel handelen en niet-intentioneel handelen. De voor dit onderzoek geselecteerde voorvallen kenmerken zich door onbedoelde (niet-intentionele) uitval van ICT-systemen in ziekenhuizen, waardoor maatregelen genomen moesten worden om schade aan patiënten te voorkomen. De gekozen afbakening van dit onderzoek hangt enerzijds samen met het feit dat er ten tijde van de start van het onderzoek in Nederland, voor zover bekend bij de Onderzoeksraad, geen voorval had plaatsgevonden waarbij een cyberaanval had geleid tot ICT-uitval in een ziekenhuis.[102] Anderzijds hangt de keuze voor de afbakening samen met het beeld dat er nog weinig aandacht is voor risico's van ICT-uitval voor de patiëntveiligheid als gevolg van niet-intentioneel handelen.[103] De Raad denkt vanuit de gekozen invalshoek een toegevoegde waarde te kunnen bieden voor digitale veiligheid

100 Deze drie begrippen vormen samen de BIV. Beschikbaarheid is hierbij de eigenschap van het toegankelijk en bruikbaar zijn op verzoek van een bevoegde entiteit (zie NEN 7510-1, p.17). Integriteit is hierbij de eigenschap van nauwkeurigheid en volledigheid (zie NEN 7510-1, p.20). Vertrouwelijkheid is hierbij de eigenschap dat informatie niet beschikbaar of niet bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen (zie NEN 7510-1, p.26).

101 Inclusief de deelverzameling topklinische ziekenhuizen.

102 In het buitenland hadden ten tijde van de start van het onderzoek wel cyberaanvallen op ziekenhuizen plaatsgevonden. In 2017 werden in Groot-Brittannië van bijvoorbeeld meerdere ziekenhuizen het slachtoffer van een ransomware aanval (de WannaCry ransomware aanval). Kort voor publicatie van dit onderzoek vond een cyberaanval plaats op een Nederlands ziekenhuis. Op 15 januari 2020 hebben hackers namelijk een poging gedaan in te breken in de digitale systemen van het Medisch Centrum Leeuwarden. Het ziekenhuis besloot daarop alle dataverkeer met de buitenwereld tijdelijk af te sluiten.

103 De Onderzoeksraad komt mede op basis van literatuurstudie en bestudering van brieven, die het ministerie van VWS in recente jaren aan de Tweede Kamer heeft gestuurd, tot de constatering dat er meer aandacht is voor security en privacy-gerelateerde vraagstukken dan voor safety-gerelateerde vraagstukken als het gaat om ICT in de zorg.

in ziekenhuizen in het algemeen, en het beheersen van risico's van ICT-uitval in ziekenhuizen voor de patiëntveiligheid in het bijzonder.

Referentiekader
De Onderzoeksraad hanteert bij zijn onderzoeken een referentiekader waarin de belangrijkste uitgangspunten voor de veiligheid betreffende het onderzoeksthema beschreven zijn. Het referentiekader vormt daarmee tevens een belangrijke basis voor de aanbevelingen. In hoofdstuk 1 van dit rapport worden de vijf uitgangspunten toegelicht die de Raad in dit onderzoek heeft gehanteerd: patiëntveiligheid, kwaliteit van zorg, verantwoordelijkheid voor het beheersen van risico's, borging van zorgcontinuïteit, en leren van incidenten.

Onderzoeksaanpak
Centraal in dit onderzoek staan de reconstructie en analyse van de drie ICT-storingen die zich hebben voorgedaan in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis. Daarvoor zijn interviews gehouden met betrokken medewerkers, is documentatie bestudeerd en zijn verschillende analysemethoden gebruikt. In totaal heeft de Onderzoeksraad circa 90 interviews gehouden, onder andere met direct bij het voorval betrokken interne medewerkers en externe partijen, met leden van de Raden van Bestuur, met vertegenwoordigers van de medische staf, managers ICT, CMIO's en CNIO's, vertegenwoordigers van klinische afdelingen en van de afdelingen kwaliteit en veiligheid. Daarnaast heeft de Raad gesproken met het ministerie van VWS en de IGJ. Naast interviews heeft de Onderzoeksraad ook een groot aantal documenten bestudeerd. Deze lopen uiteen van technische informatiedocumenten als logbestanden, netwerktekeningen, root cause analyses en Service Level Agreements[104], tot aan verslagen van crisisoverleggen, evaluatieverslagen, jaarverslagen, beleidsdocumenten, strategische documenten en kamerbrieven.

Onderzoek naar ICT-storingen
De feitenverzameling richtte zich op de oorzaak of oorzaken van de storingen, de (technische) incidentbestrijding en crisisbeheersing, de risico's van uitval van ICT voor de patiëntveiligheid en het beheersen van deze risico's.

Oorzaak storing
De Onderzoeksraad heeft op basis van interviews, documentstudie en de analyse van logbestanden met behulp van Splunk[105], getracht de directe oorzaak of oorzaken van de ICT-storingen te achterhalen. Bij het IJsselland Ziekenhuis is dit niet gelukt, omdat daarvoor niet de juiste en niet voldoende data was vastgelegd.

Om de achterliggende factoren van de ICT-storingen te kunnen blootleggen, is gekeken naar de inrichting en het beheer van het ICT-fundament in de onderzochte ziekenhuizen.

104 Een Service Level Agreement is een overeenkomst met daarin de afspraken tussen de aanbieder en de afnemer van een dienst of product. In deze overeenkomst ligt vast wat de prestatie-indicatoren en kwaliteitseisen zijn van de te leveren dienst of product, om deze later te kunnen toetsen. Een Service Level Agreement kan als afspraak bestaan tussen zowel externe (leverancier) als interne (klant) partijen binnen een organisatie.
105 Opbouw van een *Splunk instance* en de invoering van alle logbestanden ter indexatie, normalisatie, visualisatie en correlatie van events om uiteindelijk één of meerdere oorzaken van het incident aan te kunnen wijzen.

Per voorval zijn daarbij andere accenten gelegd, al naar gelang het relevant was voor het betreffende voorval. Er is dus geen sprake van een volwaardige audit van het ICT-fundament en de beheerprocessen, maar van een beschrijving en analyse op hoofdlijnen. Zowel voor het ICT-beheer als voor het ICT-fundament in de onderzochte ziekenhuizen geldt dat deze gedurende het onderzoek aan verandering onderhevig zijn geweest. De situatie zoals beschreven in dit onderzoek, stemt daarmee niet automatisch overeen met de werkelijkheid op het moment van publicatie van het onderzoek.

ICT beheer
Voor de analyse van het ICT-beheer in ziekenhuizen is gebruik gemaakt van de ISO 27002 *Information Technology Infrastructure Library*, oftewel ITIL (v3). ITIL is een reeks van best practices en concepten over het inrichten van de beheerprocessen binnen een ICT-organisatie. Het biedt een set richtlijnen, waarbij het de dienstverlening (*services*) als uitgangspunt neemt. De richtlijnen zijn ingedeeld naar de verschillende fases van de *Service Lifecycle*, waarbij de fases weer zijn opgedeeld in processen. In de praktijk bestaan ook andere handvatten voor het inrichten van ICT-beheer. Dat de Onderzoeksraad voor zijn onderzoek gebruik heeft gemaakt van ITIL, wil niet zeggen dat andere kaders niet zouden voldoen.

ICT-fundament
Voor de analyse van het ICT-fundament is uitgegaan van de volgende principes:

- Veerkracht (design voor beschikbaarheid): het fundament is bestand tegen uitval van fysieke componenten zoals kabels of andere dragers, devices, harde schijven, etc.
- Schaalbaarheid (design voor groei of pieken): het gebruik van het fundament is dynamisch en kent pieken en dalen.
- Standaardisatie: de onderdelen van het fundament zijn voor zover mogelijk gestandaardiseerd op hetzelfde type hardware, software en versie.
- Doelmatigheid: een goede architectuur bepaalt voor ieder onderdeel van het fundament de benodigde redundantie, schaalbaarheid en standaardisatie. Het fundament is afgestemd op de functionele eisen van de gebruikers en het ondersteunde proces.

Technische incidentbestrijding
De technische incidentbestrijding betreft dat deel van het onderzoek dat zich richt op de wijze waarop de ICT-afdeling - al dan niet met externe partijen en in contact met de rest van de organisatie - het incident heeft afgehandeld. Het gaat hierbij met name om het inschatten van de ernst van de storing, het alarmeren en opschalen, het verstrekken van informatie aan de crisisorganisatie, het vinden van de oorzaak en het oplossen van de storing.

Crisisbeheersing
Het onderzoek naar de crisisbeheersing richtte zich zowel op de voorbereiding op ICT-uitval als op het optreden van de crisisorganisatie tijdens de afhandeling van het incident. Het onderzoek naar de crisisbeheersing richtte zich daarbij op het verloop van de volgende processen:

- Melding en alarmering;
- Op- en afschaling;
- Leiding en coördinatie;
- Informatiemanagement;
- Crisiscommunicatie;
- Opleiden, trainen, oefenen; en
- Evaluatie.

In de rapportage is met name aandacht besteed aan die onderdelen waar volgens de Onderzoeksraad ruimte voor verbetering is. Derhalve vormen het aandachtspunten voor een adequate beheersing van risico's van ICT-uitval voor de patiëntveiligheid.

Digitalisering van de zorg en patiëntveiligheid
Voor het in kaart brengen van de digitalisering van de ziekenhuiszorg is voornamelijk literatuur bestudeerd en zijn gesprekken met deskundigen gevoerd. Voor het onderzoek naar de gevolgen voor de patiëntveiligheid zijn onder andere incidentmeldingen die betrekking hadden op de dag van de ICT-storing opgevraagd en geanalyseerd, mede met behulp van medewerkers van de betrokken ziekenhuizen.

Aanknopingspunten voor verbeteren risicobeheersing identificeren
De Onderzoeksraad heeft, vanuit de organisatorische context waarbinnen de onderzochte voorvallen plaatsvonden, aanknopingspunten geïdentificeerd om de risico's op ICT-uitval in ziekenhuizen en de gevolgen hiervan voor de patiëntveiligheid vroegtijdig in beeld te krijgen en adequaat te beheersen.

Overige voorvallen
Naast uitgebreid onderzoek naar de storingen in het Radboudumc, het IJselland Ziekenhuis en het Dijklander Ziekenhuis, heeft de Raad drie andere storingen die zich gedurende de looptijd van het onderzoek voordeden, op hoofdlijnen beschouwd. Het gaat om storingen in het Amsterdam UMC (locatie VUmc), de Noordwest Ziekenhuisgroep en het Medisch Spectrum Twente. Daartoe zijn documenten opgevraagd bij deze ziekenhuizen, zoals crisisplannen, verslagen van de crisisoverleggen, evaluatieverslagen en root cause analyses. Deze documenten zijn bestudeerd en waar nodig heeft de Onderzoeksraad aanvullende vragen gesteld om de bevindingen van de ziekenhuizen beter te kunnen duiden. Met het gebruik van de door de ziekenhuizen en extern betrokken partijen opgestelde documenten, onderschrijft de Onderzoeksraad niet automatisch de conclusies van de betrokken partijen.

De Onderzoeksraad heeft deze drie storingen beschouwd om te zien of er sprake was van overeenkomsten in de achterliggende factoren tussen de drie onderzochte en de drie beschouwde voorvallen. Dat kan er immers op duiden dat de gesignaleerde tekortkomingen en de geformuleerde lessen voor meer ziekenhuizen van toepassing zouden kunnen zijn. Een beschrijving van de oorzaak van deze storingen, de incidentbestrijding en het functioneren van de crisisorganisatie staat in bijlage F.[106] In een enkel geval wordt in voorliggend rapport naar deze voorvallen verwezen.

106 Bijlage F is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

Toelichting op bijlagen
Bij dit rapport behoren diverse bijlagen. De bijlagen A (*Onderzoeksverantwoording*), B (*Inzagereacties*) en C (*Betrokken partijen*), zijn opgenomen in het rapport en behoeven als zodanig geen toelichting. Bijlage D (*Technische onderzoeksrapportages*), E (*Analyse crisisbeheersing*) en F (*Beschrijving andere incidenten*) zijn niet opgenomen in het rapport maar staan op de website van de Onderzoeksraad. Hieronder volgt een korte toelichting op deze bijlagen.

Bijlage D bevat een uitgebreide beschrijving en analyse van de directe en achterliggende oorzaken van de voorvallen en de (technische) incidentbestrijding ervan in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis.

Bijlage E bevat uitgebreide informatie over het verloop van de crisisbeheersing bij de drie voorvallen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis.

Bij de beschrijving en analyse van het verloop van de crisisbeheersing in het Radboudumc, dient een kanttekening geplaatst te worden. De Onderzoeksraad startte zijn onderzoek naar patiëntveiligheid bij ICT-uitval in ziekenhuizen circa negen maanden nadat de ICT-storing zich in het Radboudumc had voorgedaan. Daardoor is het niet altijd mogelijk gebleken om alle details boven water te krijgen. De informatie in de bijlage is daarom voor een belangrijk deel gebaseerd op een door het Radboudumc uitgevoerde evaluatie van de ICT-storing en de interviews van de Raad met de direct betrokkenen. Gezien de tijd tussen het incident en het moment dat de gesprekken met betrokkenen hebben plaatsgevonden, is de informatie die zij konden verstrekken eveneens minder betrouwbaar dan wanneer de interviews kort na het voorval zouden hebben plaatsgevonden.

Ook in het onderzoek naar het verloop van de crisisbeheersing in het IJsselland Ziekenhuis heeft de Raad niet alle details kunnen achterhalen. Dat komt omdat er summiere verslagen van de overleggen van het crissisteam en de ICT-overleggen zijn gemaakt en er geen evaluatieverslag beschikbaar is. De beschrijving (en analyse) van de crisisbeheersing is daarom gebaseerd op beperkt beschikbare documentatie en op interviews met de direct betrokkenen.

Bijlage F bevat een beschrijving van de oorzaak, de (technische) incidentbestrijding en het verloop van de crisisbeheersing bij drie voorvallen die in 2018 en 2019 plaatsvonden in het Amsterdam UMC (locatie VUmc), de Noordwest Ziekenhuisgroep en het Medisch Spectrum Twente. De Onderzoeksraad heeft deze drie voorvallen alleen op hoofdlijnen beschreven en beschouwd. De Onderzoeksraad heeft zijn beschrijving en beschouwing opgesteld op basis van de onderzoeken die de betreffende ziekenhuizen en de door hen ingehuurde ICT-dienstverleners zelf hebben uitgevoerd. De Onderzoeksraad heeft zelf geen onderzoek gedaan naar deze incidenten en kan dus niet beoordelen of de bevindingen en analyses van deze partijen correct zijn. Dat de Onderzoeksraad deze onderzoeken heeft gebruikt om een weergave te kunnen geven van de incidenten,

betekent dan ook niet dat de Onderzoeksraad de bevindingen en conclusies in deze onderzoeken onderschrijft. Wel laten deze incidenten overeenkomstige factoren zien met de drie diepgaand onderzochte ziekenhuizen. Deze factoren betreffen met name welke keuzen er op het spel staan bij de inrichting en het beheer van het ICT-fundament, de bestrijding van ICT-uitval en de beheersing van de gevolgen van ICT-uitval voor de patiëntveiligheid. De beschrijving en beschouwing van deze ICT-incidenten dragen daarmee bij aan het formuleren van verbeterpunten in de risicobeheersing van ICT-uitval.

Begeleidingscommissie

De Onderzoeksraad heeft voor dit onderzoek een begeleidingscommissie samengesteld. Deze commissie bestond uit leden met voor het onderzoek relevante deskundigheid onder voorzitterschap van de heer Stavros Zouridis (raadslid van de Onderzoeksraad voor Veiligheid). De leden zaten op persoonlijke titel in de begeleidingscommissie. Gedurende het onderzoek is de commissie drie keer bijeengekomen om met het raadslid en het projectteam van gedachten te wisselen over de opzet en resultaten van het onderzoek. De commissie vervult een adviserende rol binnen het onderzoek. De eindverantwoordelijkheid voor het rapport en de aanbevelingen ligt bij de Onderzoeksraad. De commissie was als volgt samengesteld:

prof. dr. mr. S. Zouridis	Voorzitter Begeleidingscommissie Raadslid Onderzoeksraad voor Veiligheid
prof. dr. B. van den Berg	Hoogleraar Cybersecurity Governance, Universiteit Leiden
prof. dr. L.P.H. Leenen	Medisch afdelingshoofd Traumachirurgie UMC Utrecht, Bijzonder hoogleraar zorgkwaliteit in ziekenhuizen
prof. dr. P.L. Meurs	Buitengewoon raadslid Onderzoeksraad voor Veiligheid
dr. A.P. Nelis	Lid Raad van Toezicht ziekenhuis Rijnstate
ir. R. Prins	Buitengewoon raadslid Onderzoeksraad voor Veiligheid
prof. dr. W.J.M. Spaan	Voorzitter Raad van Bestuur LUMC, Voorzitter Nederlandse Federatie van Universitair Medische Centra

Projectorganisatie

Namens de Onderzoeksraad is voor dit onderzoek tot 1 oktober 2018 prof. mr. dr. Erwin Muller opgetreden als portefeuillehouder. Vanaf die datum heeft prof. mr. dr. Stavros Zouridis het portefeuillehouderschap van hem overgenomen. Het onderzoek is uitgevoerd door het projectteam, dat als volgt was samengesteld:

ir. G.W. Medendorp	Onderzoeksmanager
drs. S. Pijnse van der Aa	Projectleider
drs. E.J. Ettema	Onderzoeker
drs. F. van Leusden	Onderzoeker (tot 1 augustus 2019)
E.P.H. Moonen	Onderzoeker
R.J.P.N. van Schijndel MSc	Onderzoeker
Th. Cordier	Extern onderzoeker (tot mei 2019)
J. Croonenbroek	Extern onderzoeker (tot januari 2019)
ing. L.C. de Wolff	Extern onderzoeker
drs. E. Mol	Adviseur Onderzoek en ontwikkeling (tot 1 februari 2019)
drs. E.J. Willeboordse	Adviseur Onderzoek en ontwikkeling (1 februari 2019 - 1 september 2019)
dr. E.M. de Croon	Adviseur Onderzoek en ontwikkeling (vanaf 1 september 2019)
P. Boers, MA	Secretaris
A.N.J.J. Meijboom	Projectondersteuning
R. Lagendijk	Projectondersteuning

Voor het onderzoek heeft de Onderzoeksraad ook enkele experts betrokken bij het in kaart brengen van de wet- en regelgeving, het beschrijven van de digitalisering van de zorg en voor het tegenlezen van het rapport:

F.B.P. Ahsmann MSc
A.W.R. Hubert
First Lawyers

BIJLAGE B

INZAGEREACTIES

Een conceptversie van het rapport, zonder beschouwing en aanbevelingen, is, conform de Rijkswet Onderzoeksraad voor Veiligheid, voorgelegd aan betrokken partijen ter controle op feitelijke onjuistheden en onduidelijkheden.

Het conceptrapport is voorgelegd aan de volgende partijen:

- IJsselland Ziekenhuis
- Dijklander Ziekenhuis
- Radboudumc
- Medisch Spectrum Twente
- Noordwest Ziekenhuisgroep
- Amsterdam UMC (locatie VUmc)
- Bij de incidenten betrokken (door de ziekenhuizen) extern ingehuurde organisaties, leveranciers en fabrikanten.

De ontvangen reacties zijn in de volgende twee categorieën te verdelen:

- Correcties van feitelijke onjuistheden, aanvullingen op detailniveau en redactioneel commentaar heeft de Onderzoeksraad voor zover juist en relevant overgenomen. De betreffende tekstdelen zijn in het eindrapport aangepast. Deze reacties zijn niet afzonderlijk vermeld.
- De reacties die de Onderzoeksraad niet heeft overgenomen, zijn opgenomen in een tabel die te vinden is op de website van de Onderzoeksraad voor Veiligheid: www.onderzoeksraad.nl. In de tabel is tevens toegelicht waarom de reacties niet zijn overgenomen.

BIJLAGE C

BETROKKEN PARTIJEN

Bij het organiseren van ICT in de ziekenhuiszorg is een groot aantal partijen betrokken. Het gaat zowel om partijen met een systeemverantwoordelijkheid als om partijen met een meer directe verantwoordelijkheid voor het leveren van kwaliteit van zorg en voor de inrichting en werking van het ICT-fundament binnen het ziekenhuis. De taken en verantwoordelijkheden van de belangrijkste partijen die in dit onderzoek aan bod komen, worden hieronder kort beschreven.

Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Het Ministerie van VWS is verantwoordelijk voor de zorg voor de volksgezondheid. Dit betreft onder andere het beleid met betrekking tot ziekenhuizen, geneesmiddelen, ziektekosten en huisartsen. De minister voor Medische Zorg is verantwoordelijk voor een goed werkend en samenhangend stelsel voor curatieve zorg.[107, 108] Vanuit deze verantwoordelijkheid stimuleert de minister onder andere het bevorderen van de kwaliteit, (patiënt)veiligheid en innovatie in de curatieve zorg. Een stelsel van wetten, beleidsinstrumenten, toezichthouders en maatregelen dat de minister hanteert, moet bijdragen aan het bevorderen van deze belangen. Binnen het wettelijk kader kan de minister voor Medische Zorg en Sport besluiten om aanvullend beleid te voeren dat bijdraagt aan het bevorderen van kwaliteit en veiligheid in de curatieve zorg. Deze instrumenten bestaan met name uit subsidies en opdrachten.

Inspectie Gezondheidszorg en Jeugd (IGJ)
De IGJ is namens de minister van VWS de toezichthouder in de gezondheidszorg. De IGJ ziet toe op de veiligheid en kwaliteit van zorg door toezicht, handhaving en opsporing van strafbare feiten. Dit doet zij onder meer op basis van kwaliteitsstandaarden die in een openbaar register zijn opgenomen. Sinds 2018 houdt de inspectie zich tevens bezig met de toepassing van e-health.

107 Vaststelling begroting Ministerie van Volksgezondheid, Welzijn en Sport, 2019, beleidsartikel 2, curatieve zorg.
108 De primaire verantwoordelijkheid voor het leveren van kwalitatief goede en veilige zorg ligt bij zorgaanbieders, professionals en verzekeraars. Verzekeraars vallen buiten de scope van dit onderzoek.

Raad van bestuur ziekenhuis
De raad van bestuur van een ziekenhuis heeft een eindverantwoordelijkheid als het gaat om het goed organiseren van zorgverlening in instellingsverband. De raad van bestuur dient de risico's voor de patiëntenzorg te kennen en te beheersen en is eindverantwoordelijk voor de kwaliteit en de veiligheid van de zorg.[109] De opdracht voor goede zorg strekt zich naast het gebouw ook uit over de personele en materiële middelen.[110]

Medische specialisten/medische staf
Zoals de raad van bestuur verantwoordelijk is voor de kwaliteit van zorg, zo is de medisch specialist verantwoordelijk voor de juiste en goede zorg.[111] Zij leggen daarvoor verantwoording af aan de raad van bestuur. Periodiek worden binnen de medische staf incidenten, calamiteiten, complicaties, (bijna) fouten en klachten besproken en worden verbeteracties geformuleerd, uitgevoerd en periodiek geëvalueerd.

Chief information officer (CIO)
De CIO is de hoogste verantwoordelijke binnen het ziekenhuis op het gebied van de ICT. Een CIO wordt in sommige organisaties ICT-manager/directeur, manager Informatiezaken of Informatiemanagement genoemd en is onder meer verantwoordelijk voor het strategische beleid en beheer van de gemeenschappelijke informatievoorziening en de daarvoor ingezette informatiesystemen. Daartoe behoort tevens het beheer van alle hard- en software van de organisatie.

ICT-afdeling
De ICT-afdeling is doorgaans verantwoordelijk voor het ICT-fundament in een ziekenhuis. Tot de verantwoordelijkheden van de afdeling behoren onder andere de aanschaf en het beheer van alle ICT-hard- en software van de organisatie.

ICT-leveranciers
Tot ICT-leveranciers kunnen worden gerekend leveranciers van hard- en software, softwareontwikkelaars, leveranciers van ICT-management, serviceproviders, *Software as a Service* (SAAS)-providers en cloudproviders. ICT-leveranciers maken afspraken met ziekenhuizen door middel van dienstverleningsovereenkomsten, licentieovereenkomsten en *Service Level Agreements*.

Chief Medical Information Officer (CMIO) / Chief Nurse Information Officer (CNIO)
Functionaris die een brugfunctie vervult tussen ICT en de gebruiker in het ziekenhuis. Deze functionarissen leveren een bijdrage aan inbedding van technologie in de zorg en moeten zorgen voor meer verbinding tussen zorgprofessionals en informatietechnologie experts.

109 Brief IGZ aan de raad van bestuur van het Amphia ziekenhuis, 23 mei 2016, waarin zij verscherpt toezicht aanzegt.
110 Artikel 3, Veegwet VWS 2016.
111 Kwaliteitskader medisch specialisten.

De CMIO's hebben zich verenigd in een netwerk. De rol van het netwerk is naast onderlinge kennisuitwisseling ook het behartigen van de belangen van medisch specialisten richting landelijke partijen als het Ministerie van VWS, de Nederlandse Federatie van Universitair Medische Centra (NFU) en de Nederlandse Vereniging van Ziekenhuizen (NVZ), maar ook richting softwareleveranciers.

De CNIO's zijn sinds 2017 verenigd in het landelijk CNIO-netwerk. De CNIO is er op gericht om ervoor te zorgen dat zorgprofessionals in hun werk optimaal worden ondersteund door de mogelijkheden die informatisering biedt, zodat patiënten en zorgprofessionals daarvan profiteren.[112]

112 http://vzi.venvn.nl/CNIO.

ONDERZOEKSRAAD
VOOR VEILIGHEID

Bezoekadres
Lange Voorhout 9
2514 EA Den Haag
T 070 333 70 00
F 070 333 70 77

Postadres
Postbus 95404
2509 CK Den Haag

www.onderzoeksraad.nl