Bijlage D
Technische onderzoeksrapportages

Den Haag, februari 2020

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

De Onderzoeksraad heeft onderzoek gedaan naar de ICT-storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis. Deze bijlage bevat een uitgebreide weergave van het onderzoek naar de directe en achterliggende oorzaken van de storingen en de (technische) incidentbestrijding.

LIJST VAN AFKORTINGEN

BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie
CISO	Chief Information Security Officer
EPD	Elektronisch Patiënten Dossier
ICT	Informatie- en communicatietechnologie
MER	Main Equipment Room
PRI	Prospectieve Risico Inventarisatie
SLA	Service Level Agreement

LIJST VAN BEGRIPPEN

Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)
BIV staat voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. 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).

Bridge Aggregation (BAGG) errors
Foutmeldingen over een netwerkverbinding die bestaat uit meerdere gebundelde fysieke verbindingen.

Broadcastpakket
Een datapakket dat naar alle aangesloten gebruikers wordt gestuurd.

Cluster
Meerdere computers die gezamenlijk een functionaliteit invullen.

Controller (storage)
Een element in een storagesysteem dat de functie heeft om data weg te schrijven en op te halen van de opslagdisks van de storage.

CPU-load
De belasting van de Centrale Processor Unit. Dit wordt meestal uitgedrukt in een percentage van de maximale belasting.

Dimensionering
De globale ontwerpgrenzen van het systeem.

Ethernet frame
Een datapakket op laag 2 van het OSI-model.

Failover
De overschakeling van de primaire node naar de secundaire node.

Flow control
Een mechanisme dat ervoor zorgt dat verkeer (ethernet frames) gedoseerd wordt verstuurd als de ontvanger de verkeersstroom niet snel genoeg kan verwerken.

Forced takeback
Een commando waarmee de storage geforceerd wordt overgeschakeld van de ene node naar de andere node.

iSCSI host
Een host (computer) die via een netwerkprotocol (Internet Small Computer System Interface) verbinding heeft met de dataopslag (storage)

L2-netwerk
Een netwerk waarin de data op laag 2 van het OSI-model (datalink layer) wordt gerouteerd.

Loop
Een loop in een netwerk ontstaat wanneer twee punten uit een netwerk op meer dan één manier met elkaar verbonden zijn. Dit kan leiden tot het 'rondzingen' van verkeer waardoor uiteindelijk het netwerk niet langer beschikbaar is.

MAC-adres
Unieke identificatie (adres) van een netwerk interface. Binnen een L2-Netwerk wordt routering op basis van MAC-adressen gedaan.

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

OSI-model
Het OSI-model is een gestandaardiseerd referentiemodel voor datacommunicatie. Het OSI-model onderscheidt zeven lagen in datacommunicatie, die ieder een 'eigen' functioneel aspect aan de datacommunicatie beschrijven. Laag 1 gaat over de fysieke media die voor datatransmissie kunnen worden gebruikt en bevat bijvoorbeeld de elektrische en optische specificaties voor bits en transmissiesnelheden. Laag 7 betreft de applicatielaag waar de communicatie met de eindgebruikers wordt gedefinieerd. Alle tussenliggende lagen voegen ieder hun eigen functionaliteit toe, waarbij laag 2 zorgt voor transport van de data over een verbinding.

Pauze frame
Een ethernet frame dat aangeeft dat de ontvanger de aangeboden verkeersstroom niet kan verwerken.

Pingen
Het versturen van een datapakket naar een host. Dit pakket zal over het algemeen door de host worden beantwoord met een ICMP-reply, waardoor de netwerkverbinding te controleren is op goede werking.

Prospectieve Risico Inventarisatie (PRI)
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.

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

Service level agreement (SLA)
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.

Spanning Tree Protocol
Een mechanisme dat in het gehele netwerk ervoor zorgt dat er geen dubbele verbindingen mogelijk zijn tussen de bestemmingen van het netwerk en dat er zo naar alle bestemmingen in een netwerk één pad beschikbaar is.

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

Storagearchitectuur
Het globale ontwerp en dimensionering van een storagesysteem.

Switch
Een netwerkapparaat dat data kan schakelen op basis van MAC-adres.

System integrator
De organisatorische eenheid die verantwoordelijk is voor de geïntegreerde werking van een systeem.

Virtualisatie
Bij virtualisatie worden meer besturingssystemen op één hardwareserver gedraaid. Daarmee wordt optimaal gebruik gemaakt van die ene server. Ook het beheer en onderhoud beperkt zich tot één enkele machine.

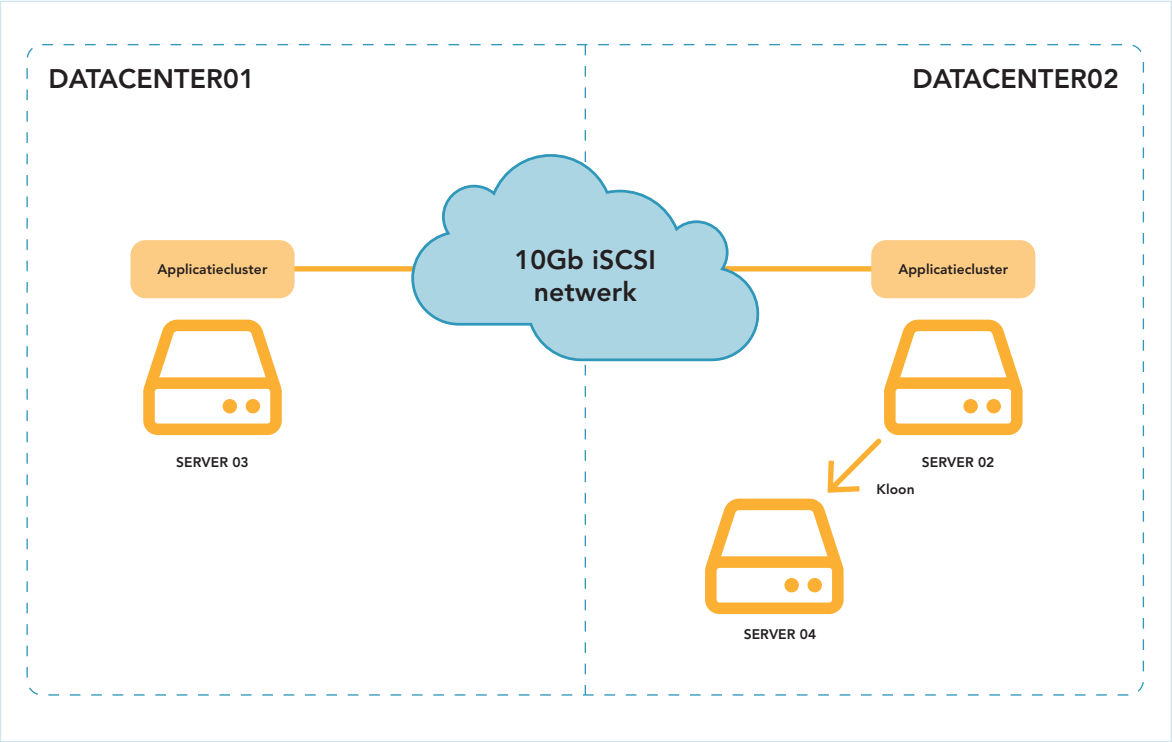
Virtual machine
Een softwarematig gecreëerde machine (server) waarop programma's kunnen worden uitgevoerd.

D.1 Radboudumc

D.1.1 Beschrijving toedracht

Op 26 januari 2018 om 09:56 uur maakte een ICT-medewerker van het Radboudumc een kopie van een virtual machine[1]. Dit zogenaamde 'klonen' werd uitgevoerd in de grafische interface van de VMWARE[2]. De virtual machine die de medewerker trachtte aan te maken, betrof een iSCSI host[3].[4] De bedoeling was om de gekloonde host onderdeel te laten worden van een cluster. Het betrof een cluster dat voor testredenen was gecreëerd. Een cluster bestaat uit twee identieke machines die elkaar kunnen overnemen in geval van hardware falen. In dit geval bestond het cluster uit de machines SERVER02[5] en SERVER03 die respectievelijk in datacenters DATACENTER01 en DATACENTER02 stonden. De reden voor het klonen was dat de virtual server SERVER03 qua configuratie niet correct te krijgen was. Om te vermijden dat langdurig gezocht moest worden naar de fouten in de configuratie, is besloten een kloon van de wel goed werkende server (SERVER02) te maken en deze als vervanging voor SERVER03 in te zetten. De gekloonde server werd SERVER04 genoemd.

1 Een virtual machine is een softwarematig gecreëerde machine (server) waarop programma's kunnen worden uitgevoerd.
2 VMWARE is een commerciële naam voor een bepaald type virtualisatiesoftware.
3 Een iSCSI host is een host (computer) die via een netwerkprotocol (Internet Small Computer System Interface) verbinding heeft met de dataopslag (storage).
4 RCA van fabrikant 6 april 2018.
5 De echte namen van alle ICT-elementen die in deze bijlage worden genoemd zijn bekend bij de Onderzoeksraad. Om veiligheidsredenen zijn deze namen in dit stuk geanonimiseerd.



Figuur D1: Klonen van een testserver.

Behalve dat er in de VMWARE een server werd gekloond, diende deze gekloonde server ook bekend te worden gemaakt in de storage[6] als vervanging van server SERVER03. SERVER04 werd daarom bekend gemaakt binnen de storage. Deze actie bleek echter niet volledig te worden uitgevoerd. Er dienden als gevolg van dit bekendmaken twee databasetabellen te worden aangepast. Door een softwarefout werd echter maar één van deze tabellen aangepast. In de andere tabel werd de nieuwe host niet opgenomen. De ICT-medewerker was zich hier echter niet van bewust, omdat de grafische interface geen melding hierover terugkoppelde naar deze medewerker.

Hierdoor ontstond er een inconsistentie tussen de databases van het systeem die de actieve configuratie voor de beide locaties administreerden. De ontstane situatie met een inconsistentie tussen twee databasetabellen is niet toegestaan in het systeem, omwille van bescherming van data-integriteit. Op het moment dat de gekloonde server data van de storage opvroeg, merkte de storagesoftware deze inconsistentie op. De inconsistentie werd door het systeem geïnterpreteerd als een fout van de node (controller[7]) waarna een herstart werd gegeven. Omdat dit de inconsistentie in de database niet verhielp, gebeurde hetzelfde nogmaals. Na een aantal herstarten deactiveerde de software de controller en bracht deze in een service-status zodat diagnosedata verzameld kon worden.[8] Het systeem is uitgerust met in totaal vier controllers. Omdat één controller uitviel, nam de tweede controller automatisch de taken van de falende controller over. Doordat het falen een gevolg was van een inconsistentie

6 De systemen die bedoeld zijn om digitale gegevens in op te slaan.
7 Een element in een ICT-systeem dat de functie heeft om data weg te schrijven en op te halen van de opslagdisks van de storage.
8 Dit deactiveren is het gevolg van een aanhoudend probleem, waardoor de normale operatie van de node wordt gestaakt en de node in service-status wordt gebracht.

in beide databases welke (tevens) garant staan voor data-integriteit, herhaalde ditzelfde scenario zich voor de tweede tot en met de vierde controller. Daarmee was er op enig moment geen actieve controller meer over om de data in DATACENTER01 te bereiken. Dit gold niet alleen voor de (virtual) servers van het testcluster, maar voor alle servers die van de primaire storage van het datacenter DATACENTER01 gebruik maakten (ruim tweehonderd).[9] De volumes die wel beschermd werden door redundantie-technieken, waren bereikbaar vanaf DATACENTER02.

Om 10:33 uur maakte de ICT-afdeling van het Radboudumc een service request aan naar aanleiding van het wegvallen van de storagefunctionaliteit in DATACENTER01. In een telefonisch contact tussen de fabrikant van de storage (vanaf hier: de fabrikant) en het Radboudumc, vroeg de fabrikant het Radboudumc snapshots van het systeem te maken en deze op te sturen voor verdere analyse. De fabrikant alloceerde een engineer. Die was om 13:30 uur ter plaatse om de storing verder te analyseren. Tegelijkertijd werd er een problem report aangemaakt. De situatie werd als ernstig geschat en de fabrikant schaalde meteen maximaal op om technische ondersteuning aan het Radboudumc te leveren. Level 3 support van de fabrikant werd geactiveerd, die op haar beurt de loggings deelde met ontwikkelaars voor verdere analyse.

De supportgroep van de fabrikant achterhaalde niet lang daarna de oorzaak van het falen en stuurde rond 17:15 uur een workaround om de controllers weer online te krijgen. Alle vier de controllers van DATACENTER01 zijn in korte tijd na elkaar herstart, dit om de storageomgeving (de controllers) weer actief te krijgen. Deze actie gaf het gewenste resultaat, de storage werd weer beschikbaar. Daarop kwamen alle virtuele servers op de storage weer online. In die situatie is de betreffende corrumperende server uitgeschakeld om verdere problemen te voorkomen.

Nadat de workaround was gevonden waarbij de inconsistentie in de database in ieder geval niet zou kunnen leiden tot uitval van de controllers, moest een softwarepatch worden geschreven om het ontstaan van een dergelijke inconsistentie in de toekomst te voorkomen. Om te achterhalen wat de oorzaak was van het optreden van de inconsistentie, werden testen uitgevoerd in een testomgeving. Dit resulteerde erin dat op 23 maart 2018 de condities waaronder deze fout optreedt, konden worden gereproduceerd. Daarmee kon ook de softwarepatch voor deze fout in de software worden geschreven. Deze patch kwam beschikbaar op 5 april 2018.[10]

D.1.2 Analyse toedracht

Het incident werd veroorzaakt door een softwarefout in de storage. De fout werd geactiveerd door een activiteit van de beheerder. De activiteit betrof het klonen van een testserver en het daarna actief maken van de gekloonde server en het toekennen van storagevolumes aan dit gekloonde systeem. Al deze activiteiten zijn normale handelingen die in een productieomgeving kunnen worden uitgevoerd.

9 Analyse rapport RCA.
10 RCA van fabrikant 6 april 2018.

In algemene zin kan gesteld worden dat wijzigingen in een productieomgeving zijn toegestaan, mits deze de bestaande actieve gebruikers van de storage maar niet beïnvloeden of substantiële risico's voor deze actieve gebruikers inhouden. Handelingen als software-updates zijn daarom in de regel niet zondermeer toegestaan in een productieomgeving.

De betreffende virtual machine behoorde tot een testcluster en was daarmee niet actief in het primaire proces (de zorg voor patiënten) van het Radboudumc. De gevolgen van de softwarefout in de storage maakte echter wel dat de primaire storage in datacenter DATACENTER01 volledig onderuit ging. Dat het klonen van een server dergelijke gevolgen zou kunnen hebben, had redelijkerwijs niet door het personeel van het Radboudumc kunnen worden voorzien.

Er is snel gereageerd op het optreden van de storing. Tussen het vaststellen van de storing (rond 10:15 uur) en het aanmaken van de severity-1 call bij de fabrikant, zat 15 minuten. Het ICT-personeel heeft daarmee de ernst van de situatie correct ingeschat. Ook de fabrikant nam de melding serieus en schakelde meteen het *Enhanced Technical Team* in. Voor eventueel ter plaatse benodigde acties werd een support engineer naar het Radboudumc gestuurd. Omdat het probleem geen hardwarefalen betrof, was de reparatietijd uit de service level agreement (SLA)[11] niet van toepassing.[12] Toch wist de fabrikant rond 17:00 uur dat een database-inconsistentie de oorzaak van de uitval was en, belangrijker, had de fabrikant een workaround die de storagefunctionaliteit weer herstelde. Gezien de complexiteit van de omgeving en de aard van de storing (*softwarefalen*) kan worden vastgesteld dat de storing professioneel is opgepakt en de workaround spoedig is gevonden.

D.1.3 Analyse techniek

Achtergrond
Voor de storage maakte het Radboudumc gebruik van vijf systemen van dezelfde fabrikant. Op één van deze systemen (de zogenaamde primaire storage) trad de storing op. De primaire storage fungeerde als de standaardoplossing voor dataopslag als geen andere oplossing vanwege specifieke eisen nodig is.[13] Bij de invulling van het systeem werden drie typen disks toegepast. Het verschil tussen deze disks is dat ze óf worden geoptimaliseerd op snelheid, óf op capaciteit óf een combinatie van deze elementen.

11 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.
12 Service overeenkomst fabrikant.
13 Storage architectuur 2015-2020.

Het doel van het systeem is dat de binnenkomende data automatisch op de benodigde opslagperformance wordt geclassificeerd en daarna aan de volumes met de best passende performancekarakteristieken wordt toegekend. Een performancecategorie[14] wordt in dit verband een tier genoemd en het automatisch indelen van de data wordt autotiering genoemd.

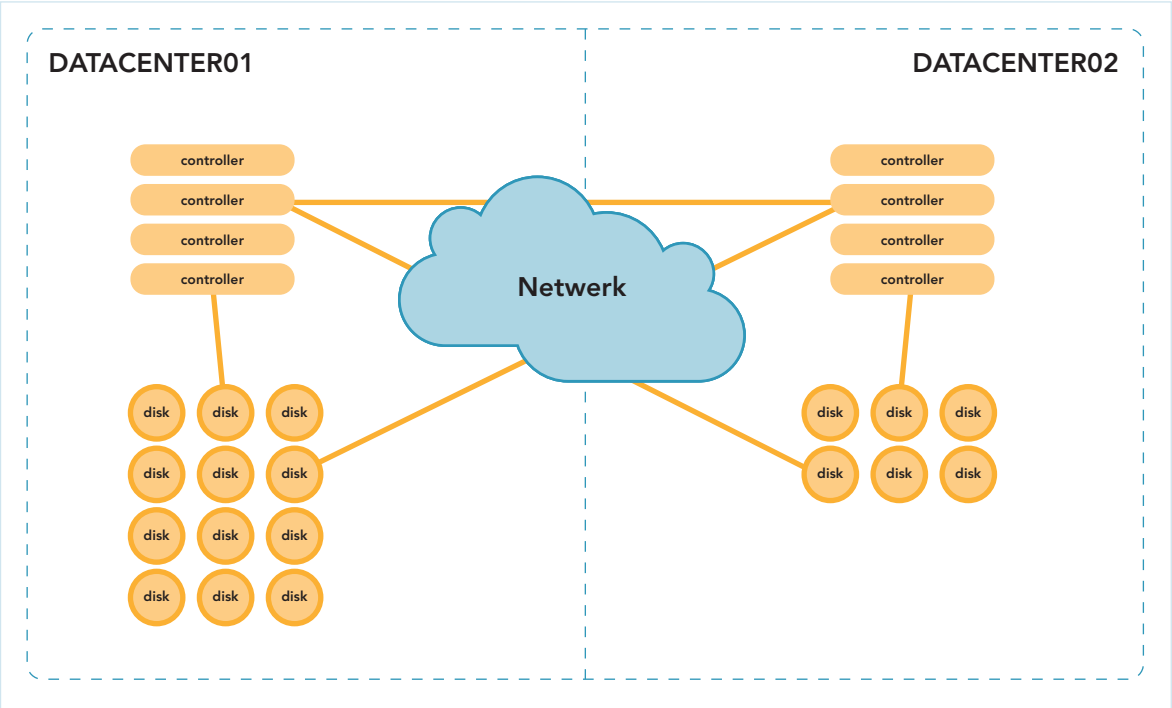
In totaal worden er drie performancecategorieën gedefinieerd:

Tier 1: *High performance tier*: met zeer snelle disks.
Tier 2: *Performance tier*: voor de minder performance kritische data.
Tier 3: *Capacity tier*: voor data die niet of nauwelijks gebruikt wordt.

De primaire storage van Radboudumc betreft een systeem dat is geplaatst in twee geografisch gescheiden datacenters (datacenterlocaties DATACENTER01 en DATACENTER02). Het systeem bevat vier controllerparen, twee paar op iedere locatie. De controllers verzorgen het schrijven en lezen naar de opslagdisks (volumes). Het systeem is geschikt om de data gerepliceerd weg te schrijven over de twee geografisch gescheiden locaties. In dit geval zijn dat de beide datacenters. Bij uitval van een volledige locatie kan de data nog benaderd worden op de tweede locatie.

In de storageconfiguratie van het Radboudumc was ervoor gekozen om de opslagcapaciteit tussen de twee locaties verschillend te maken. Ook werd er nog geen gebruik gemaakt van de mogelijkheid om de data gerepliceerd weg te schrijven over de twee geografisch gescheiden locaties. Hierdoor was de geografische redundantie, zoals deze door de storage kan worden geboden, niet beschikbaar in de configuratie van het Radboudumc. De reden hiervoor was dat het eerdere systeem ook geen datareplicatie over twee datacenters bood en ervoor gekozen was om eerst het systeem zonder verdere wijzigingen te migreren naar de (nieuwe) primaire storage en pas daarna nieuwe features als datareplicatie toe te voegen. Deze keuze stemde daarmee in ieder geval tijdelijk niet overeen met de vastgestelde storagearchitectuur[15], waarbij voor kritische data was vastgesteld dat deze gerepliceerd moest worden.

14 Een verzameling van media met een gelijke performance.
15 De storagearchitectuur is het globale ontwerp en dimensionering van een storagesysteem.



Figuur D2: Schematisch overzicht storagesysteem.

Verder is er bij de dimensionering[16] van het systeem rekening mee gehouden dat datacompressie zou worden toegepast. Hierbij was het uitgangspunt dat er minimaal 20% opslagruimte zou kunnen worden bespaard.[17]

Het incident met de storage vond plaats in een context waarbij er discussie was over de performance van het systeem (de primaire storage) tussen het Radboudumc en de leverancier van de storage. De performance van het systeem speelde echter geen rol bij de verstoring of de duur daarvan.

Datareplicatie

Het incident had voorkomen kunnen worden indien de data gerepliceerd was geweest over twee datacenters (DATACENTER01 en DATACENTER02). Geodatareplicatie op de storage was echter niet volledig in gebruik, met uitzondering van het testplatform. In de aanbestedingsdocumenten wordt hierover gezegd dat de functionaliteit van datareplicatie op diverse niveaus kan worden gerealiseerd. Dit zijn achtereenvolgend: applicatieniveau, databaseniveau, OS-niveau, VMWare niveau en storageniveau.[18] Van het storageniveau is zeker dat dit niet werd gebruikt.[19] Gezien de uitval van systemen is duidelijk dat de andere niveaus ook onvoldoende actief waren.

Onbalans in de primaire storage

De primaire storage kende een onbalans in de geboden opslagcapaciteit. De opslagcapaciteit van DATACENTER01 was ruim twee maal zo groot als de capaciteit van DATACENTER02. Dit houdt in dat datareplicatie in ieder geval niet voor alle data kon worden gerealiseerd.

16 Dimensionering betreft de globale ontwerpgrenzen van het systeem.
17 Uitvraag Radboudumc aanvullende brief van 31 maart 2016.
18 Storage architectuur 2016-2020, 16 februari 2016.
19 Holistic storage review fabrikant, 7 december 2018.

Het houdt ook in dat er een onbalans was in de belasting van de controllers in de beide datacenters. Bij toepassing van datareplicatie zal daarmee rekening moeten worden gehouden. De fabrikant en de leverancier adviseerden een dergelijke configuratie niet.[20]

Aanbesteding system integrator[21] storage
In aanloop naar de aanbesteding van de storage is een intern onderzoek naar de bestaande ICT-infrastructuur van het Radboudumc uitgevoerd. Hieruit kwam naar voren dat circa 80% van de infrastructuur van het Radboudumc niet voldoende was ingevuld. Naar aanleiding van deze bevinding is besloten om een verbeterprogramma te starten waarbij per onderdeel concrete verbeteracties zijn geformuleerd. Eén van die acties was het aanbesteden voor een system integrator die alle benodigde hardwaremerken kon leveren. Het doel was om later in samenwerking met deze system integrator de hardwareleverancier door middel van een nieuwe aanbesteding te selecteren. In het model dat uiteindelijk is gebruikt, werd een additionele implementatiepartner geselecteerd. Daardoor is er naast de integrator ook nog een extra implementatiepartner in de keten toegevoegd. Hierdoor kon er een situatie ontstaan waarin een duidelijke onderlinge verantwoordelijkheidsverdeling ontbrak. Deze partijen moesten gezamenlijk wel een geïntegreerde infrastructuur leveren. Het leveren van een dergelijke omgeving door verschillende partijen met een onduidelijke verantwoordelijkheidsverdeling, kan leiden tot (spraak)verwarring.

Complexiteit van de omgeving
De ICT-omgeving van het Radboudumc kent over de tijd heen een centralisatie van techniek. Servers zijn gevirtualiseerd en centraal in hardwareclusters gerealiseerd, de storage is gecentraliseerd, netwerken worden geïntegreerd en voor verschillende doelen gebruikt, etc. De voordelen zijn evident: gevirtualiseerde werkplekken vereenvoudigen bijvoorbeeld sterk het beheer ervan. Tegelijkertijd maakt het de impact van een storing potentieel veel groter. De uitval van een dergelijk gecentraliseerd platform kan meteen veel gebruikers raken.

> Bij virtualisatie worden meer besturingssystemen op één server gedraaid. Daarmee wordt optimaal gebruik gemaakt van die ene server. Ook het beheer en onderhoud beperkt zich tot één enkele machine.

In relatie tot de storage kan worden opgemerkt dat hier een veelheid van functionaliteit samenkomt, waardoor het beheren van de storage een complexe, gespecialiseerde taak is. De aangetroffen functionaliteit betrof hier: het op verschillende manieren repliceren van data, het optimaliseren van het systeemgebruik naar performance-eisen van data en het comprimeren van data. Hoewel deze functionaliteit in isolatie gebruikt zijn nut kan hebben, verhoogt het combineren van al deze mogelijkheden het risico op onverwachte effecten op de performance van het systeem en/of de uiteindelijke beschikbare

20 Holistic storage review fabrikant, 7 december 2018.
21 Een system integrator is een organisatie(eenheid) die verantwoordelijk is voor de geïntegreerde werking van een systeem.

functionaliteit van het systeem. Dit vergt zorgvuldige inrichting en beheer van de storageoplossing en vergt de beschikbaarheid van voldoende gekwalificeerde resources binnen de ICT-afdeling om hier bij voortduring adequate invulling aan te geven.

D.1.4 Analyse beheer

Event management en incident management

Zoals al eerder is vastgesteld, was de reactie op de verstoring van de storage zeer snel en is ook vrijwel direct bij de leverancier een prioriteit-1 melding gemaakt. Ook aan de kant van de leverancier is meteen actie ondernomen. Dit heeft geresulteerd in een voor dit type verstoring spoedige oplostijd.

Capacity management

Capacity management van storage is een complexe aangelegenheid met veel parameters. Hier een gewogen ontwerpbeslissing in nemen, vergt een grondig inzicht in de gebruikers van een systeem, hun wensen en vooral de ontwikkeling over tijd daarin. Een te strakke invulling van de initiële vraag kan later tot performanceproblemen leiden vanwege onverwachte knelpunten in de geleverde hardware.

Met betrekking tot capacity management is in de aanbestedingsdocumenten van Radboudumc voor de storage een groeiprognose voor 2016 tot 2020 afgegeven.[22] In 2017 werd echter een uitbreiding besteld die qua verwerkingssnelheid buiten de originele prognose viel. Uit een review eind 2018 bleek dat de primaire storage ondanks deze uitbreiding op piekmomenten overbelast werd.

IT service continuity management

IT service continuity management richt zich op de uitzonderlijke situatie dat normale maatregelen gefaald hebben en de continuïteit van bedrijfskritische processen geraakt wordt. Het incident met de primaire storage was zo'n type incident. De normale maatregelen om de beschikbaarheid van de storage te garanderen faalden, omdat het hier om een softwarefout ging die de storage van een heel datacenter uitschakelde. Dit is vergelijkbaar met het effect van een brand in het datacenter.

Voor de inschatting van de eisen die een applicatie stelt aan beschikbaarheid, integriteit en vertrouwelijkheid wordt de BIV-classificatie[23] gebruikt. Bij deze classificatie worden applicaties ingedeeld op hun eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. Conform de door Radboudumc gehanteerde maatregelen BIV-classificaties[24] zou de data van een kritische applicatie met betrekking tot beschikbaarheid moeten worden gerepliceerd over twee datacenters. Dat dit niet voor alle kritische applicaties is gebeurd, blijkt uit problemen met GLIMS, de laboratoriumapplicatie die, als gevolg van de storage-uitval, niet meer functioneerde. Dit zorgde ervoor dat het laboratorium over moest gaan op de noodprocedure. De verwerkingscapaciteit van het

22 Bijlage E: Storage architectuur 2016-2020, 16 februari 2016.

23 BIV staat voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. 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).

24 Bijlage C: BIV maatregelen, architectuurprincipes en strategiekeuzes Storage Architectuur 2016-2020.

laboratorium viel sterk terug. De uitval van GLIMS verstoorde de normale operatie van het ziekenhuis zodanig, dat een opnamestop moest worden afgekondigd.

Samenvattende conclusie
De ICT-uitval in het Radboudumc werd veroorzaakt door een softwarefout, die optrad tijdens het uitvoeren van werkzaamheden in de productieomgeving van de storage van het ziekenhuis. Deze werkzaamheden betroffen handelingen die redelijkerwijs in de productieomgeving mogen worden uitgevoerd. Het optreden van de softwarefout was niet te voorzien geweest.

De softwarefout in de storage raakte niet alleen de toegang tot de data van de server die de fout triggerde, maar ook de toegang tot de data van alle servers die van de storage gebruik maakten in DATACENTER01. Doordat deze data niet geografisch gerepliceerd was over de twee datacenters, was de impact van de storing voor het primaire proces van het ziekenhuis substantieel.

Na vaststelling van de storing is er zowel door het personeel van het Radboudumc als de fabrikant spoedig en adequaat gehandeld. Dit heeft ervoor gezorgd dat de downtijd van de storage minimaal is gebleven.

D.2 IJsselland Ziekenhuis

D.2.1 Beschrijving toedracht

In de nacht van 2 op 3 juni 2018 belde om 01:25 uur een medewerker van de receptie de dienstdoende systeembeheerder van het IJsselland Ziekenhuis. De receptiemedewerker meldde dat er sprake was van een telefoniestoring en dat de SAP-applicatie niet werkte. Een paar minuten later ontving de externe leverancier, die het netwerk in beheer had, een automatische melding van de telefoniestoring.

De systeembeheerder voerde testen uit en constateerde dat de e-mail nog functioneerde, maar dat er problemen waren met de SAP-applicatie, dat er veel meldingen in Zabbix[25] stonden en dat het niet lukte om in te loggen op sommige servers. Deze servers waren wel te pingen[26]. Dat betekent dat er nog wel een fysieke verbinding was.

Omstreeks 01:55 uur die nacht deed het ziekenhuis voor het eerst formeel melding van de netwerkstoring bij de externe leverancier. De leverancier constateerde dat alle uplink verbindingen tussen de core en server/access switches[27] weer up waren. Alle switches waren bereikbaar. Het netwerk was traag, maar in de switches waren geen problemen zichtbaar. De leverancier communiceerde dit niet (duidelijk) naar het ziekenhuis,

25 Zabbix is een open source monitoring applicatie voor netwerken en applicaties.
26 Pingen is het versturen van een datapakket naar een host. Dit pakket zal over het algemeen door de host worden beantwoord met een ICMP-reply ,waardoor de netwerkverbinding te controleren is op goede werking.
27 Een switch is een netwerkapparaat dat data kan schakelen op basis van MAC adres (laag 2 OSI model).

waar nog altijd sprake was van problemen, omdat servers waren uitgeschakeld naar aanleiding van de netwerkstoring. De leverancier was niet op de hoogte van de problemen in het ziekenhuis. Hij dacht dat alle problemen waren verholpen. De systeembeheerder van het ziekenhuis verwachtte dat de leverancier onderzoek zou gaan doen naar de storing en hem zou informeren wanneer hij de servers weer kon gaan opstarten. Eén en ander werd echter niet naar elkaar toe gecommuniceerd.

Even later vroeg de dienstdoende systeembeheerder een andere beheerder met meer kennis van het netwerk om naar het ziekenhuis te komen om te helpen. Via een WhatsApp -groep werden leidinggevenden en systeembeheerders geïnformeerd over de storing. Belangrijke gebruikers werden door hun eigen leidinggevende geïnformeerd.

De ICT-medewerkers van het ziekenhuis besloten in overleg met een vertegenwoordiger van de raad van bestuur van het ziekenhuis om de applicatieservers nog niet op te starten, maar te wachten op de reactie van de leverancier. De leverancier had zoals gezegd niet in de gaten dat het ziekenhuis wachtte op zijn akkoord. Ondertussen was de leverancier een onderzoek gestart naar de oorzaak van de storing en besloot op aandringen van het IJsselland Ziekenhuis op te schalen en een senior network engineer naar de storing te laten kijken.

Omstreeks 05:00 uur 's nachts besloot de dienstdoende systeembeheerder om zoveel mogelijk systemen uit te schakelen en/of uitgeschakeld te houden om dataverlies tegen te gaan. Om 06:20 uur werd duidelijk dat het ziekenhuis door een miscommunicatie al een paar uur wachtte op groen licht van de leverancier om de servers opnieuw op te starten, terwijl de leverancier zich hier niet van bewust was. Na telefonisch contact tussen de ICT-medewerkers van het ziekenhuis en de leverancier kwam dit misverstand naar voren en besloot men om alle servers weer op te starten.

Omstreeks 11:00 uur bekeek een technisch specialist van het ziekenhuis de logging van de firewall om te controleren of er wellicht sporen te vinden waren van een aanval, maar hij ontdekte geen bijzonderheden. Men constateerde een probleem met het inloggen op thuiswerkplekken en de dienstdoende systeembeheerder schakelde daarop de twee factor authenticatie tijdelijk uit, zodat artsen en andere dienstdoende gebruikers de systemen weer konden raadplegen.[28] Ondertussen werden logfiles verzameld en verzonden. Het was inmiddels 12:00 uur toen de service engineer networking van de externe leverancier telefonisch contact had met het ICT-team van het IJsselland Ziekenhuis. Alle servers waren herstart en de leverancier voerde testen uit op het netwerk. Om 13:30 uur was er opnieuw telefonisch contact tussen de twee partijen. Alles leek naar behoren te werken en de storing werd na een korte telefonische evaluatie afgemeld.

D.2.2 Analyse toedracht

De analyse van de toedracht valt uiteen in een analyse van de oorzaak van de storing en een analyse van de incidentbestrijding. Beide analyses komen in deze paragraaf aan bod.

28 Deze is dezelfde dag weer aangezet.

Oorzaak

De directe oorzaak van de storing is te herleiden tot een probleem met het netwerk. Uit de analyse van logbestanden blijkt namelijk dat de verbindingen in het netwerk van het IJsselland Ziekenhuis uitvielen. Dat is terug te vinden in de logfiles van de switches waar de volgende meldingen zichtbaar waren:

Tijdframe	Systeem	Foutmeldingen
1:21:26 –1:26:25	Network	'Netwerk BAGG errors' & 'STP topology changes'

Tabel D1: Melding uit logfile switch.

De logfiles tonen aan dat verbindingen tussen servers en switches uitvielen en het gehele netwerk voor een periode van vijf minuten niet operationeel was. Doordat er geen verbinding meer was tussen een groot aantal servers, waren applicaties die op deze servers draaiden niet langer beschikbaar voor gebruikers.

De foutmeldingen en dan met name de melding 'STP[29] topology change' in combinatie met de waarneming dat alle apparatuur in het netwerk niet meer kon communiceren over het netwerk, duidt erop dat er een loop[30] in het netwerk was opgetreden. Een ongecontroleerde loop in een L2-netwerk[31] zorgt ervoor dat over het netwerk na verloop van tijd geen communicatie meer mogelijk is. Spanning Tree Protocol is bedoeld om die gevolgen van een loop te ondervangen. Dit doet het protocol door gecontroleerd verbindingen in het netwerk uit te zetten.

Bridge Aggregation (BAGG) errors[32] geven aan dat delen van het netwerk die bestaan uit meerdere fysieke verbindingen (zogenaamde gebundelde verbindingen) niet meer werken.

Spanning Tree Protocol is een mechanisme dat in het gehele netwerk ervoor zorgt dat er geen dubbele verbindingen mogelijk zijn tussen de bestemmingen van het netwerk en dat er zo naar alle bestemmingen in een netwerk één pad beschikbaar is. Een Spanning Tree Protocol 'topology change' betekent dat de netwerkpaden opnieuw berekend worden. Tijdens de herberekening is het netwerk niet beschikbaar.

29 Hiermee wordt Spanning Tree Protocol afgekort.
30 Een loop in een netwerk ontstaat wanneer twee punten uit een netwerk op meer dan één manier met elkaar verbonden zijn. Dit kan leiden tot het 'rondzingen' van verkeer waardoor uiteindelijk het netwerk niet langer beschikbaar is.
31 Een L2-netwerk is een netwerk waarin de data op laag 2 van het OSI-model (datalink layer) wordt gerouteerd.
32 Foutmeldingen over een netwerkverbinding die bestaat uit meerdere gebundelde fysieke verbindingen.

Stabiele verbindingen tussen applicatie- en storageservers zijn om twee redenen van belang:

- Applicaties gebruiken storage om gegevens op te slaan. Het opslaan of "wegschrijven" van gegevens is een kritiek proces dat onmiddellijk verstoord raakt indien een netwerkverbinding meer dan dertig seconden niet beschikbaar is. Om te voorkomen dat gegevens verloren gaan of niet overeenstemmen, worden applicaties gesloten of opnieuw opgestart als er sprake is van een netwerkstoring.
- Virtuele (applicatie)servers maken gebruik van de hardware die ze door de virtualisatiesoftware ter beschikking wordt gesteld voor hun rekencapaciteit en netwerkverbindingen. Ze gebruiken storageservers voor het opslaan van belangrijke bestanden, hun besturingssysteem en voor schrijfruimte. Daarom is ook hier een stabiele netwerkverbinding nodig om te zorgen dat de virtuele (applicatie)servers goed kunnen functioneren. Als in dit proces een netwerkverbinding wegvalt, moeten deze servers handmatig of automatisch opnieuw worden opgestart om te kunnen blijven functioneren. In het geval van het IJsselland Ziekenhuis zijn sommige servers uit zichzelf afgesloten. Anderen zijn door de systeembeheerder uitgezet. Het is niet duidelijk welke servers automatisch zijn uitgezet en welke handmatig zijn afgesloten. Dit is niet uit de beschikbare logfilebestanden op te maken.

Dit verklaart de gevolgen van de netwerkstoring voor de gebruikers, namelijk dat applicaties niet beschikbaar waren. Door het verlies van de verbinding tussen storage- en applicatieservers moesten servers opnieuw worden opgestart om de applicaties weer in gebruik te kunnen nemen. Het ICT-team van het ziekenhuis werkte daarbij samen met de applicatiebeheerders om te controleren of alles weer naar behoren functioneerde. Het opstarten van de verschillende servers heeft veel tijd in beslag genomen. Dit is op zich niet ongebruikelijk, maar er zijn indicaties dat dit proces sneller uitgevoerd had kunnen worden als er betere communicatie was geweest tussen de externe leverancier die verantwoordelijk was voor het beheer van het netwerk en het ICT-team in het ziekenhuis.

Gezien het feit dat de serverproblemen zijn ontstaan na de storing op het netwerk, lijkt het erop dat deze storing ook de directe oorzaak is van de problemen. Netwerken zijn over het algemeen zeer stabiel en het is niet uitzonderlijk dat een netwerk 100% beschikbaar is over een periode van jaren, afgezien van stroomstoringen.

Waarom het netwerk in storing raakte, kan niet met zekerheid worden gesteld. Uit onderzoek van de logfilebestanden en gesprekken met de betrokken medewerkers van de ICT-afdeling en leveranciers zijn twee mogelijke scenario's naar voren gekomen die de storing kunnen verklaren. Deze verklaringen sluiten elkaar overigens niet volledig uit. Het is voorstelbaar dat beide scenario's zich hebben voorgedaan, tegelijkertijd of zelfs in direct verband met elkaar.

Mogelijke oorzaak: pauze frames en flow control
De netwerkleverancier beschrijft in zijn root cause analyse[33] dat de storing is veroorzaakt door het flow control protocol. Dit protocol zou pauze frames hebben verstuurd.[34] Ook de fabrikant van de switches beschrijft dat flow control hier waarschijnlijk de oorzaak is geweest.

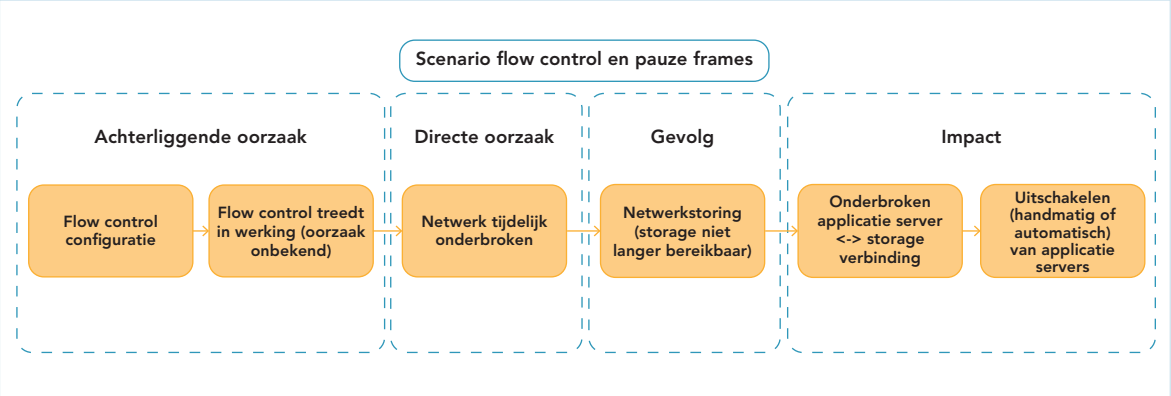
Flow control is een mechanisme dat ervoor zorgt dat verkeer (ethernet frames[35]) gedoseerd worden verstuurd als de ontvanger de verkeersstroom niet snel genoeg kan verwerken. Daardoor lopen de buffers die hiervoor zijn vol en dreigt er verkeer te worden 'gedropped'. De ontvangende switch kan door middel van een pauze frame aangeven dat de zendende switch zijn verkeerstroom tijdelijk moet stoppen. Doordat de buffers van de zendende switch in een dergelijk geval vol zullen lopen, zal deze ook weer een pauze frame naar haar bron sturen. Zodoende propageert het pauze frame door het netwerk totdat het bij de bron van het verkeer aankomt. Het probleem met flow control is dat al het verkeer op een interface wordt gestopt, waarmee ook het managementverkeer wordt geraakt. Onderdeel van het managementverkeer zijn de pakketjes waarmee Spanning Tree Protocol controleert of alle bestemmingen nog bereikbaar zijn. Wanneer dit managementverkeer niet meer verstuurd kan worden doordat flow control dit tegenhoudt door middel van een pauze frame, dan kan dit een Spanning Tree Protocol topolopy change veroorzaken.[36]

> *Ethernet Flow Control* is een protocol om de hoeveelheid data die tussen verschillende netwerkapparaten verstuurd wordt te reguleren. Het probleem met dit protocol is dat het betrekking heeft op alle soorten data: ook datastromen die een normale werking van het netwerk mogelijk maken, zoals verschillende soorten managementprotocollen, worden gereduceerd of gestopt. Het netwerk kan dan tijdelijk niet beschikbaar zijn, omdat deze managementprotocollen niet meer werken. Daarom gebruikt de nieuwere versie van flow control, genaamd *Priority Flow* Control, een mechanisme om data te reduceren afhankelijk van hun prioriteit in het netwerk. Het verwijdert in eerste instantie alleen data die minder prioriteit hebben. Op die manier kan worden voorkomen dat pauze frames een geheel netwerk verstoren.

De reden waarom dit scenario als een mogelijke oorzaak van de netwerkstoring wordt aangemerkt, is dat in de logfiles van de switches veel pauze frames zijn geteld. Bij deze logfile entries staan echter geen tijdstippen, waardoor het niet met zekerheid is vast te stellen dat deze pauze frames daadwerkelijk ten tijde van het incident werden verstuurd of dat dit al weken of maanden daarvoor is gebeurd. Het aantal pauze frames wordt in een teller simpelweg opgeteld zonder dat zichtbaar is wanneer ze zijn verstuurd.

33 Een root cause analyse is een systematische aanpak om de oorzaak van een probleem of gebeurtenis op te sporen.
34 Root Cause Analyse (RCA) 1.1.
35 Een ethernet frame is een datapakket op laag 2 van het OSI-model (data link layer).
36 De technische verklaring hiervoor is dat management verkeer voor Spanning Tree Protocol en LACP niet meer kan worden verstuurd of ontvangen en dat daarom verbindingen (link bundles) niet meer beschikbaar zijn en het netwerk de beschikbare verbindingen opnieuw in kaart heeft gebracht (spanning-tree topology recalculation). Deze aanpassing van het netwerk heeft vier minuten geduurd en nadien was het netwerk weer beschikbaar.

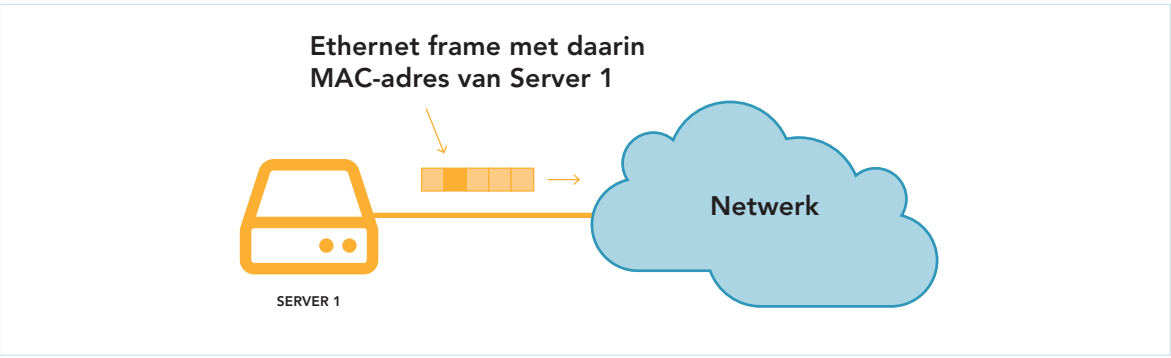
Waarom flow control in werking is getreden en wat de mogelijke hoge volumes aan data heeft veroorzaakt, kon niet worden achterhaald. Gegevens over het volume aan verkeer op het netwerk worden door de leverancier en het ziekenhuis niet verzameld of bijgehouden. Men denkt dat de storageapparatuur mogelijk overbelast raakte door een verkeerde configuratie of door onverwacht dataverkeer wegens het maken van een automatische back-up. Volgens ICT-medewerkers van het ziekenhuis zijn echter geen andere back-ups gemaakt dan gebruikelijk. Meetgegevens om dit te controleren waren niet beschikbaar. In de onderstaande afbeelding is bovenstaand scenario grafisch weergegeven.



Figuur D3: Grafische weergave scenario flow control en pauze frames.

Mogelijke oorzaak: netwerkloop

Een ander mogelijk scenario is dat de netwerkstoring werd veroorzaakt door een loop in het netwerk. Een loop ontstaat doordat een switch (onbedoeld) twee of meer mogelijkheden heeft om een bestemming te bereiken. Om te begrijpen wat er precies gebeurt, moet even kort stil worden gestaan bij de werking van een L2-netwerk.

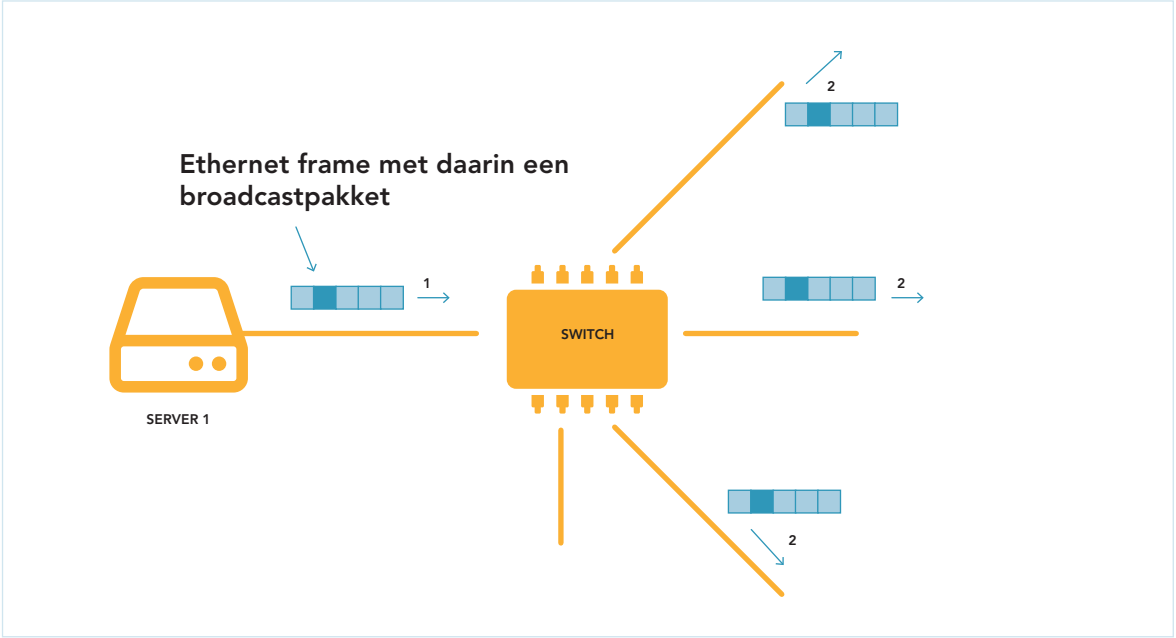


Figuur D4 Ethernet frame met daarin het MAC-adres van server 1.

Binnen een L2-netwerk wordt gebruik gemaakt van netwerkswitches die de ethernet frames (met daarin de IP-pakketjes) van zender naar ontvanger sturen. Dit versturen wordt gedaan op basis van het MAC-adres[37] van de aangesloten apparatuur. Ieder apparaat (bijv. computer, server) met een netwerk interface, stuurt op dit interface ethernet frames uit met zijn eigen MAC-adres. Naast het eigen MAC-adres wordt ook

37 Een MAC-adres is een unieke identificatie (adres) van een netwerk interface. Binnen een L2-netwerk wordt routering op basis van MAC-adressen gedaan.

het MAC-adres van de geadresseerde meegestuurd in het ethernet frame. Als dit laatste adres echter onbekend is, dan wordt een broadcastpakket[38] uitgestuurd. Dit pakket komt binnen op de switch van het netwerk waarop (in dit voorbeeld) Server 1 is aangesloten. Deze ontvangende switch zal het broadcastpakket naar al zijn overige interfaces kopiëren en uitsturen. In de reguliere situatie zal de juiste ontvanger (die op één van de interfaces is aangesloten) een pakketje terugsturen om kenbaar te maken wat zijn MAC-adres is.

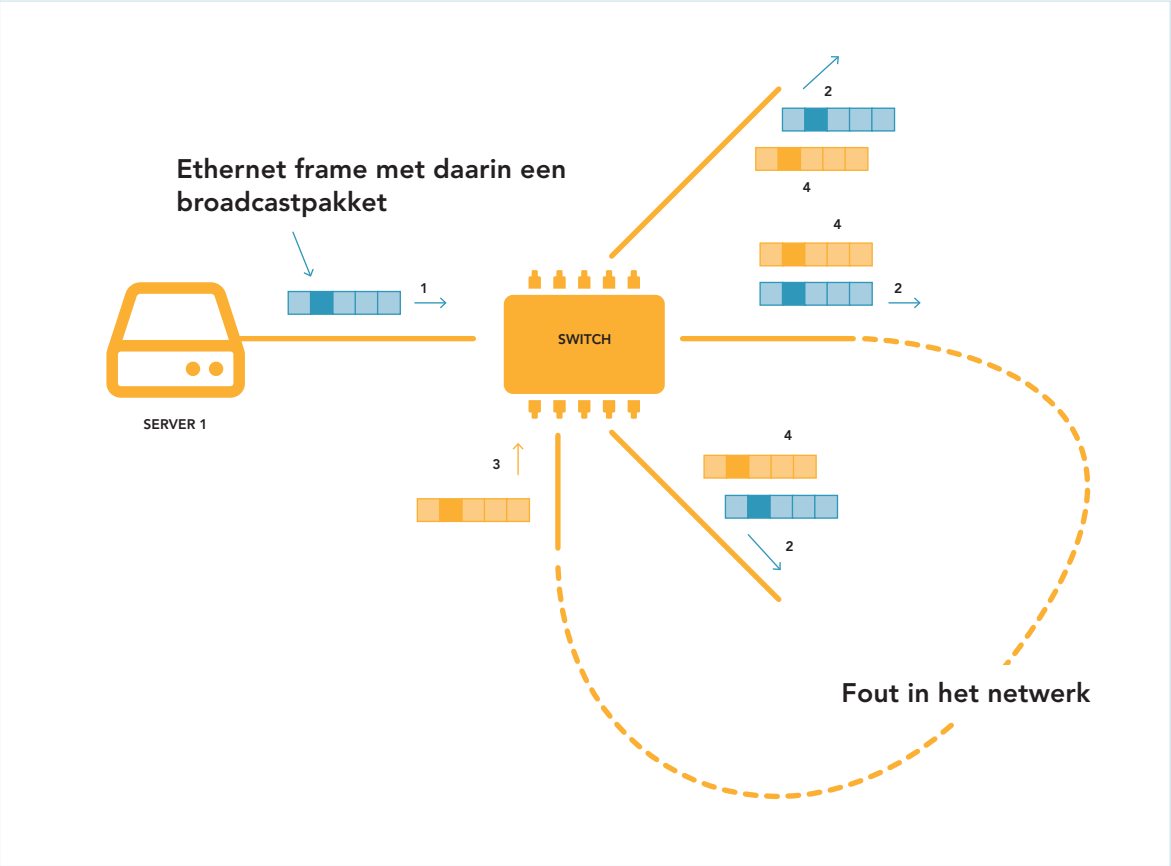


Figuur D5 Ethernet frame met daarin een broadcastpakket.

Wanneer er echter door een fout in de configuratie van het netwerk een lus in het netwerk zit waardoor een switch het door zichzelf gestuurde broadcastpakket weer ontvangt, zal ook dit pakketje weer naar alle interfaces worden doorgezet met weer

38 Een broadcastpakket is een datapakket dat naar alle aangesloten gebruikers wordt gestuurd.

hetzelfde resultaat: hetzelfde pakketje komt nogmaals binnen. Hierdoor zal het netwerk zeer snel overbelast raken met (nutteloze) broadcastpakketten. Het overige verkeer kan niet meer afgehandeld worden waardoor communicatie over het netwerk onmogelijk wordt. Dit fenomeen noemt men ook wel een '*broadcast storm*'.



Figuur D6 Ethernet frame met daarin een broadcastpakket - met een fout in het netwerk.

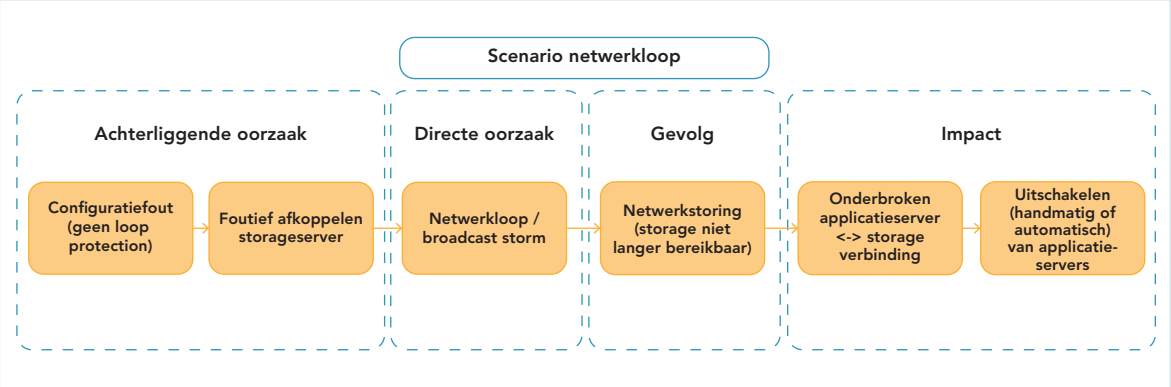
Om netwerken te beschermen tegen dit soort loops, is het mogelijk om switches zo te configureren dat het ontstaan ervan wordt tegengehouden door middel van zogenoemde '*loop protection*'. Loop protection kan netwerkloops voorkomen en is bij grotere of complexere L2-netwerken sterk aan te bevelen (de gevolgen van een netwerkloop zijn immers substantieel). In het IJsselland Ziekenhuis was geen gebruik gemaakt van loop protection.

De dag voor het incident was het IJsselland Ziekenhuis begonnen met de migratie van de storageomgeving. De oude storageserver is daarbij uitgeschakeld, maar niet losgehaald van het netwerk. Doordat de storageserver meerdere netwerkaansluitingen had, is het mogelijk dat er een loop is ontstaan. Dit probleem was bekend bij het ziekenhuis en was in het verleden al eerder geconstateerd bij een gelijksoortige handeling op het netwerk. Desondanks is de server na de migratie niet afgekoppeld van het netwerk.

Doordat het ziekenhuis geen gebruik maakte van loop protection, kon het uitzetten van de oude storageserver, zonder deze fysiek los te maken van het netwerk, een loop

veroorzaken. Indien loop protection wel was ingeschakeld, was de kans op een loop afgenomen. De externe leverancier, die in de praktijk verantwoordelijk is voor het beheer van het netwerk, is de aangewezen partij om loop protection in te schakelen. Uit het onderzoek is niet duidelijk geworden waarom dit niet is gebeurd.

In figuur D7 is het scenario grafisch weergegeven.



Figuur D7 Grafische weergave scenario netwerkloop.

Verband tussen de mogelijke scenario's
Het is mogelijk dat beide scenario's zich tegelijkertijd hebben voorgedaan. Zo zou het kunnen dat de migratie een loop veroorzaakt heeft door de afwezigheid van loop protection. Hierdoor kan een broadcast storm hebben gezorgd voor een toename in het volume van dataverkeer op het netwerk. Door deze toename kan het flow control protocol in werking getreden zijn en pauze frames hebben verstuurd. Door deze pauze frames kon managementverkeer tussen switches niet meer plaatsvinden en zou een netwerkstoring kunnen zijn ontstaan. Met zekerheid kan echter worden gesteld dat Spanning Tree Protocol is gaan herconfigureren en zeker is ook dat dit tot gevolg had dat het netwerk tijdelijk niet beschikbaar was. Dit niet beschikbaar zijn van het netwerk had op haar beurt weer het waargenomen effect op de virtuele (applicatie)servers.

Incidentbestrijding
De analyse van het incident op 3 juni 2018 geeft een indicatie van de inrichting van de incidentbestrijding in het IJsselland Ziekenhuis. Onderstaand wordt dit besproken aan de hand van de volgende aspecten: voorbereiding, detectie, analyse, inperking, bestrijding, herstel en nazorg.

Voorbereiding
Het ziekenhuis had op het gebied van beleid en procedures diverse documenten die konden bijdragen aan een goede voorbereiding op incidenten en de continuïteit van de ICT-voorzieningen. Als onderdeel van het zorgcontinuïteitsplan was een scenario voor ICT- en netwerkgerelateerde incidenten opgenomen. Daarnaast waren er procedures voor incident management. Aan de vereiste van een actuele BIV-lijst was voldaan. Een BIV-lijst helpt met het bepalen van kritische systemen die met hogere prioriteit dienen te worden behandeld.

Het beleid, de procedures en documentatie over incident management en incidentbestrijding waren echter niet centraal beschikbaar en niet op een consistente

wijze bekend in de organisatie. Niet alle medewerkers van de ICT-afdeling waren op de hoogte van alle procedures en beleidsstukken. De incident managementprocedures zijn tijdens het incident niet gebruikt.

SLA's en documentatie van de verschillende ICT-systemen werden bewaard. De ICT-medewerkers hadden toegang en konden deze informatie raadplegen wanneer nodig.

De beschikbaarheid van het ICT-team in het ziekenhuis was beperkt. De spreiding van kennis en expertise was minimaal. Dat kan ertoe leiden dat er bij uitval van personeel moeilijkheden kunnen ontstaan bij de opvang van werkzaamheden, waaronder gedurende de incidentbestrijding. Het team had verschillende expertises (zoals netwerk specialisme, firewall specialisme) waardoor afhankelijkheden ontstaan. Tijdens het incident was degene met de meeste expertise over het afhandelen van een dergelijk incident met verlof. Het gevolg hiervan was dat een ander ICT-teamlid de leiding moest nemen in de bestrijding van het incident. Ondanks de verschillen in expertise draaiden alle ICT-medewerkers (waak)diensten buiten kantooruren. Er werd wel contact gezocht met niet-dienstdoende medewerkers indien expertise nodig was, maar dit gebeurde niet op basis van formele afspraken.

Detectie
Het incident werd gedetecteerd door zowel eindgebruiker(s) als ook door een geautomatiseerde melding in de bewaking van de externe leverancier. De melding die ontvangen werd voor dit incident betrof alleen een gevolg (symptoom) van de netwerkstoring, namelijk een verstoring van de telefonie. Er waren bij de betreffende beheerders geen meldingen[39] bekend over de andere verstoringen die optraden als gevolg van de netwerkstoring: zo hadden zij niet de directe beschikking over geautomatiseerde meldingen over welke servers of applicaties last hadden en beschikten zij ook niet over de meldingen van de netwerkapparaten zelf. De storingsmeldingen werden door het systeem automatisch per mail naar de beheerders gestuurd, maar door het ontbreken van 24/7 monitoring van de systemen in het ICT-fundament werd alleen de storing van het telefoniesysteem opgemerkt.

Analyse
De externe leverancier kwam in een vroeg stadium in actie en nam ongeveer zes minuten na de automatische melding van een telefoniestoring contact op met de receptie van het IJsselland Ziekenhuis. De externe leverancier controleerde aan het begin van de storing diverse malen de netwerkstatus en koppelde daarover terug naar het IJsselland Ziekenhuis.

De analyse van de leverancier dat het om een kortstondige netwerkstoring ging was correct en deze analyse was relatief vroeg afgerond (tegen 03:00 uur in de nacht). Deze analyse is niet meteen met het IJsselland Ziekenhuis gedeeld. Het is niet bekend waarom de leverancier dit niet (duidelijk) aan het ziekenhuis heeft gecommuniceerd. Als gevolg

39 Het is belangrijk een verschil te maken tussen gebeurtenissen (events), meldingen (alarms) en incidenten (incidents). Events zijn enkel veranderingen in een systeem. Alarms zijn events die actie vereisen en onderdeel zijn van een bewakingssysteem (monitoring system). Incidents zijn storingen en meestal is een incident het gevolg van een melding.

daarvan is de verdere incidentbestrijding verlopen op basis van onvolledige informatie. Het ziekenhuis veronderstelde dat de externe leverancier een bericht zou geven zodra het ziekenhuis kon beginnen met herstelwerkzaamheden (herstarten en opstarten van servers en diensten). De externe leverancier was niet op de hoogte dat het ziekenhuis op hun toestemming wachtte. Als gevolg hiervan bleef het ziekenhuis langer in de inperking- en bestrijdingsfase dan nodig. Deze miscommunicatie heeft ertoe geleid dat de incidentbestrijding drie uur langer heeft geduurd dan nodig. Op basis van de analyse had men om 03:00 uur in de nacht met herstelwerkzaamheden kunnen beginnen, nu is dat rond 06:00 uur gebeurd.

Inperking
Er zijn geen voorzieningen of maatregelen getroffen om de gevolgen van het incident voor de gebruikers te mitigeren. In het geval van een incident zoals deze zijn inperkingen van de gevolgen mogelijk, maar niet zonder voorbereiding en investeringen. Mogelijke opties zijn de opslag van gegevens op een andere locatie (off-site back-up) die rechtstreeks te benaderen is door de applicaties op die uitwijklocatie opnieuw te installeren en via een andere verbinding toegankelijk te maken.

Bestrijding
Dat er sprake was van een storing werd relatief snel ontdekt, waarna er vrij spoedig contact was tussen het ziekenhuis en de externe leverancier die verantwoordelijk is voor het netwerk. Door de beschikbaarheid van een dienstdoende systeembeheerder kon het ziekenhuis snel acteren nadat de eerste signalen over de problemen binnen waren gekomen. Het mobiliseren van additionele kennis en medewerkers binnen het IJsselland Ziekenhuis ging voortvarend; ondanks het tijdstip in het weekend zijn diverse medewerkers actief betrokken geweest bij de afhandeling van de storing.

Tijdens de incidentbestrijding zijn applicatieservers down gebracht en/of gehouden wat in de context van het incident niet nodig was. Door het handmatig down houden van applicatieservers zijn bepaalde services vanuit het ziekenhuis niet of minder beschikbaar geweest. Het is niet duidelijk om welke services het precies gaat, omdat niet duidelijk is welke servers zijn uitgezet/automatisch uitgeschakeld zijn en welke niet. Daardoor is het niet mogelijk om precies aan te geven wat de impact op de zorg is geweest van het uitschakelen en/of handmatig down houden van de servers.

De communicatie tussen het ziekenhuis en de leverancier was niet optimaal: de impact van het incident was niet direct duidelijk bij de externe leverancier en ICT-medewerkers van het ziekenhuis hebben enkele malen moeten aandringen op acties, waaronder het opschalen naar een senior netwerk engineer. Doordat de externe leverancier het netwerk in hun controles als beschikbaar zag en geen zicht had op applicaties en servers van het ziekenhuis, konden ze niet alle gevraagde ondersteuning leveren. In een later stadium was de dienstdoende systeembeheerder in de veronderstelling dat de externe leverancier een onderzoek zou uitvoeren op het netwerk en terugkoppeling zou geven aan het ziekenhuis, waarna het ziekenhuis de applicatieservers weer op zou starten. Waarom de systeembeheerder die veronderstelling had, is niet duidelijk geworden uit het onderzoek. De externe leverancier was hier niet van op de hoogte en daardoor heeft het ziekenhuis gewacht op een signaal dat niet kwam.

Tijdens de incidentbestrijding was geen sprake van duidelijke regievoering vanuit de ICT-afdeling van het ziekenhuis. Er is geen centraal overzicht van de genomen acties of één eigenaar die het gehele incident managementproces overzag. Een mogelijke verklaring hiervoor is dat de werknemer die normaal gesproken verantwoordelijk was voor dit proces verlof had en zijn rol tijdelijk door een minder ervaren werknemer werd overgenomen.

Herstel
Het herstel verliep traag doordat het opstarten van servers geheel handmatig moest gebeuren en alleen in samenwerking tussen twee medewerkers kon plaatsvinden. De interactie met de applicatiebeheerders van de verschillende zorgafdelingen voor het testen van alle applicaties heeft daarnaast ook veel tijd in beslag genomen. Idealiter zijn processen zoals het herstarten van servers en het testen van applicaties geautomatiseerd.

Nazorg
Het ziekenhuis heeft een aantal acties uitgevoerd tijdens de nazorg van het incident. De leverancier is gevraagd om een root cause analyse te maken en verbeteringen voor te stellen. Daarnaast zijn er gesprekken gevoerd met de leverancier om verbeteringen in de samenwerking in het beheer en tijdens incidenten te verbeteren. Het definiëren van conclusies en verbeteringen bleef beperkt, omdat de oorzaak van het incident niet met zekerheid kon worden vastgesteld. Daartoe ontbraken gegevens uit loggings of monitoring die hadden kunnen helpen om te begrijpen wat er precies gebeurd is en of alle genomen acties tijdens de incidentbestrijding adequaat waren.

D.2.3 Analyse techniek
In het onderzoek van de Raad is geanalyseerd of en in welke mate er bij de inrichting van het ICT-fundament bepaalde principes (of best-practices) zijn toegepast. Omdat het onderzoek geen diepgaande analyse van het ICT-fundament van het IJsselland Ziekenhuis omvatte, is de analyse op hoofdlijnen uitgevoerd overeenkomstig de in bijlage A genoemde principes.

In het ICT-fundament van het IJsselland Ziekenhuis was overall sprake van redundantie. Zo waren veelal twee onafhankelijke verbindingen en stroomaansluitingen aanwezig, werd gebruik gemaakt van fysiek redundante paden en waren de hardware voor het centrale netwerk en de servers verdeeld over twee verschillende ruimtes (Main Equipment Room (MER))[40].

Het netwerk was opgebouwd uit drie lagen (access, distributie en core). Een dergelijke opbouw is een standaard design keuze die voldoet aan geaccepteerde *best-practices*. Het past in het principe van een modulaire opbouw die het makkelijk maakt om nieuwe capaciteit bij te schakelen. De netwerkcapaciteit van de hardware en verbindingen was normaal, met minimaal 1Gbps, en kan worden geschaald door middel van netwerkaggregatie[41] tot 80Gbps in het centrale deel van het netwerk. Dit zijn gebruikelijke

40 Een MER is een ruimte waarin centrale ICT-apparatuur is opgesteld.
41 Verschillende methodes zijn hier toegepast: meerdere verbindingen worden logisch 'bij elkaar opgeteld' tot een verbinding met grotere snelheid (*link aggregation*) of meerdere switches zijn logisch tot een switch geïntegreerd (*switch stacking*).

capaciteiten voor een organisatie van deze omvang, maar de groeimogelijkheid met de huidige hardware is beperkt. Verdere opschaling zal de aankoop van nieuwe hardware vereisen.

De hardware building blocks (modules) waren gestandaardiseerd op hetzelfde type hardware en gebouwd uit standaard componenten.
Het netwerk was doelmatig, gezien de eisen van het IJsselland Ziekenhuis. Uit de beschikbare documentatie waren duidelijke eisen met betrekking tot beschikbaarheid (>99.99%), schaalbaarheid of standaardisatie gesteld en ingevuld.[42] Wel is op te merken dat de eisen voor beschikbaarheid en schaalbaarheid alleen voor de netwerkapparatuur waren beschreven, en niet voor het netwerk als geheel (systeemeisen).

D.2.4 Analyse beheer

De belangrijkste bevindingen uit de analyse van het ICT-beheer in het IJsselland Ziekenhuis worden toegelicht in de volgende alinea's.

Change management
Het uitschakelen van de oude storage is niet gegaan volgens de best practices voor change management. Er was geen changedocumentatie aanwezig of beschikbaar en de dienstdoende systeembeheerder was niet op de hoogte dat de change had plaatsgevonden. Daarnaast was de change verkeerd uitgevoerd doordat de server uitgezet is, maar niet van het netwerk afgekoppeld was. Dit is een bekend risico voor het ontstaan van netwerkloops.

Supplier management
De communicatie tussen de ICT-afdeling van het IJsselland Ziekenhuis en hun externe leverancier tijdens het incident was gebrekkig en heeft geleid tot vertraging bij het oplossen van het incident. Doordat de beheerder van het ziekenhuis op een terugkoppeling van de medewerker van de leverancier wachtte, terwijl deze hier niet van op de hoogte was, zijn acties om de applicaties weer in gebruik te nemen veel later genomen dan noodzakelijk was.

In het algemeen constateert de Raad dat de rollen en wederzijdse verantwoordelijkheden tussen het ICT-team van het ziekenhuis en de externe leverancier ontoereikend gedefinieerd en beschreven waren. Dit is mogelijk ook een onderliggende reden waarom een fout in de configuratie (het ontbreken van loop protection) na overname van het netwerk door de leverancier niet eerder is gezien en gerepareerd.

Event management
De bewaking (monitoring) van de ICT-omgeving in het ziekenhuis was minimaal en ontoereikend om het onderzochte incident goed te kunnen bestrijden. Belangrijke gebeurtenissen waren geen onderdeel van de bewaking. Zo waren gebeurtenissen in de netwerkapparatuur en beschikbare gegevens niet op een overzichtelijke en toegankelijke manier aan elkaar gekoppeld.

42 IJsselland Ziekenhuis As-Built Network Design Document v.1.5 en Pakket van Eisen Uitbreiding Netwerk YSL.

Service level management
Met betrekking tot service level management zijn er twee belangrijke bevindingen. De eerste bevinding is dat er geen overzicht was over welke applicaties (zorgprocessen) via welke servers draaiden. Daardoor kon niet goed vastgesteld worden welke servers betrokken waren en op welke wijze deze met elkaar verbonden waren. De aanwezige kennis van de servers, applicaties en hun onderlinge relaties, bevond zich verspreid over de ICT-beheersers en de leverancier. Tijdens de crisis had geen van de aanwezige beheerders een volledig overzicht tot zijn beschikking.

De tweede bevinding is dat er geen prioritering bestond tussen de verschillende ICT-systemen en -applicaties in relatie tot de zorgprocessen. De afdeling ICT hanteerde daarom ook geen heldere prioritering bij het oplossen van incidenten en er waren geen speciale ICT-voorzieningen (back-up, extra redundantie, uitwijk) voor de belangrijkere zorgprocessen aanwezig. Tijdens het oplossen van incidenten werd een onduidelijke volgorde van activiteiten aangehouden in plaats van gestructureerd de applicaties voor de belangrijkste zorgprocessen eerst te laten functioneren.

Samenvattende conclusie
Het incident in het IJsselland Ziekenhuis betrof een netwerkstoring met als gevolg dat een groot aantal ICT-applicaties tijdelijk niet meer beschikbaar was. De zorgprocessen die afhankelijk waren van deze applicaties werden verstoord of moesten worden stilgelegd.

De oorzaak van de netwerkstoring is niet met zekerheid vast te stellen, maar kwam waarschijnlijk voort uit een tijdelijke overbelasting in combinatie met een verkeerde configuratie. De hierdoor veroorzaakte netwerkstoring heeft slechts enkele minuten geduurd, maar had een langdurige ICT-uitval tot gevolg. Een misverstand tussen het IJsselland Ziekenhuis en hun netwerkleverancier zorgde er namelijk voor dat het herstel pas drie uur later kon beginnen. Daarnaast heeft het herstel van de applicaties zelf zes uur lang geduurd, omdat de daarvoor benodigde werkzaamheden handmatig door een beperkt aantal medewerkers kon worden uitgevoerd. Uiteindelijk heeft een korte netwerkstoring een lange uitval van applicaties en lange verstoring van het zorgproces tot gevolg gehad.

De rollen en wederzijdse verantwoordelijkheden tussen het ICT-team van het ziekenhuis en de netwerkleverancier waren ontoereikend gedefinieerd en beschreven. Dit heeft er mogelijk toe geleid dat een fout in de configuratie (het ontbreken van loop protection) na overname van het netwerk door de leverancier niet eerder is gezien en gerepareerd en mogelijk (dit is één van de twee mogelijke oorzaken) heeft geleid tot het voorval.

Het IJsselland Ziekenhuis monitorde het ICT-systeem in beperkte mate, waardoor er beperkt informatie over de oorzaak en achtergronden van de ICT-storing beschikbaar was. Dit stond een goede incidentbestrijding in de weg en zorgde er ook voor dat er achteraf geen lessen geleerd konden worden over de technische oorzaken van het incident.

D.3 Dijklander Ziekenhuis – locatie Hoorn

D.3.1 Beschrijving toedracht

De ICT-storing die op 16 juli 2018 het Dijklander Ziekenhuis (locatie Hoorn) trof, is een gevolg van werkzaamheden die op die dag in de MER plaatsvonden. Vanwege koelingsproblemen in de MER was het noodzakelijk dat de daar aanwezige verhoogde vloer verder zou worden opgehoogd. In de voorbereiding van deze werkzaamheden werd besloten om de vloer, met alle daarop staande en werkende apparatuur, op te hogen. Om dit te kunnen doen, werd een gespecialiseerd bedrijf in de arm genomen. Die zette voor dit doel geëigende gereedschappen in om het ophogen probleemloos uit te kunnen voeren. Voor dit gespecialiseerde bedrijf was het vijzelen van werkende apparatuur een bekende activiteit die zij met regelmaat uitvoerde.

Enkele maanden voorafgaand aan het verhogen van de vloer in de MER, werd op initiatief van het ziekenhuis een Prospectieve Risico Inventarisatie (PRI)[43] opgesteld. Bij het opstellen van de PRI waren zowel medewerkers van het ziekenhuis betrokken, als medewerkers van de bij de werkzaamheden betrokken externe partijen. De risicomanager stelde deze PRI vast op 21 februari 2018.[44] Na deze datum werd de begintijd van de werkzaamheden bepaald op circa 16:00 uur, omdat op dat tijdstip de meeste poliklinieken en operatiekamers al gesloten zouden zijn.

Op 16 juli 2018 werd om circa 12:00 uur een kick-off gehouden tussen degenen die de werkzaamheden zouden uitvoeren en het begeleidende personeel van het ziekenhuis. Van de werkzaamheden zelf was geen draaiboek opgesteld, maar de externe opdrachtnemer vertoonde wel een zelfgemaakt voorbeeldfilmpje van het vijzelen van operationele apparatuur racks. Het vijzelen zelf werd hierbij gezien als de risicovolle activiteit die om 16:00 uur zou worden gestart. De voorbereidende werkzaamheden werden niet als risicovol gezien en werden eerder die dag gestart.

Direct na de kick-off startte het bedrijf met de voorbereidende activiteiten van het vijzelen. Deze voorbereidingen hielden in dat er draagbalken in de operationele racks werden gemonteerd om deze racks later te kunnen opvijzelen. De racks waarmee begonnen werd, bevatten de storageserver. Dit was cruciale apparatuur voor het primaire proces van het ziekenhuis, omdat hierop onder andere de database van het Elektronisch Patiënten Dossier (EPD) draaide. De gevolgen van een mogelijke uitval van deze apparatuur waren echter onbekend bij het uitvoerend personeel.[45]

Eén van de racks bleek geen ruimte voor de draagbalken te bieden in het rack zelf, waarna voor dit rack de draagbalken onder het rack werden aangebracht. Om voldoende ruimte onder het rack te creëren, draaiden de medewerkers de stelpootjes waarop het rack stond, maximaal uit. Dit rack (waar de draagbalken onder worden gemonteerd) was het rack met de controller van de storageserver. Omdat het rack met de controller (zelfs

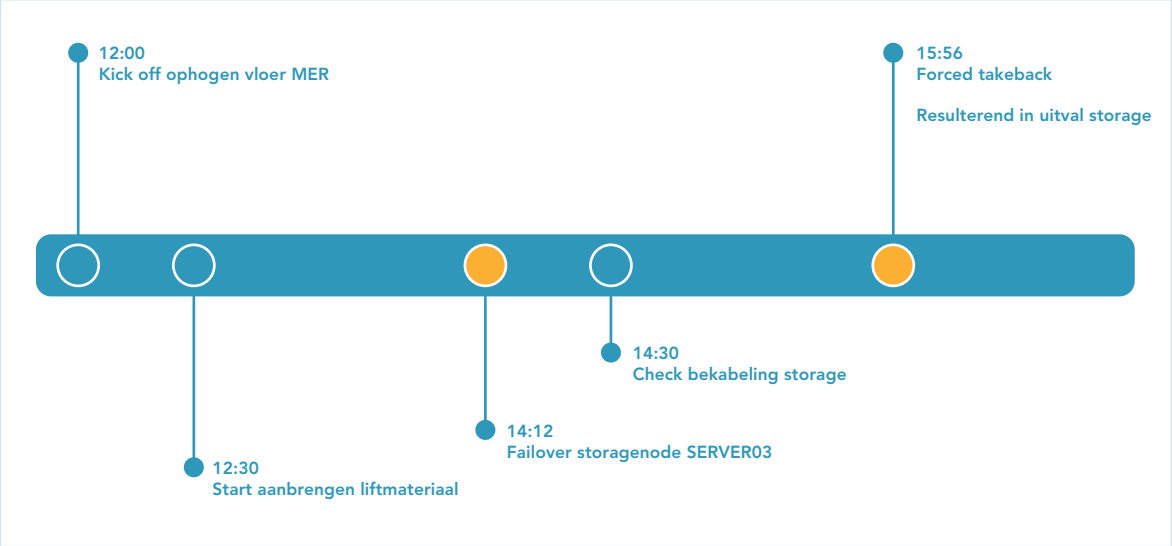
43 Een Prospectieve Risico Inventarisatie is een middel om voor risicovolle processen de risico's gestructureerd inzichtelijk te maken en voor de grootste risico's zoveel mogelijk mitigerende maatregelen te nemen.
44 Eindrapportage WFG, 25 oktober 2018.
45 Eindrapportage WFG, 25 oktober 2018.

met uitgedraaide pootjes) te dicht bij de vloer zat, moest dit rack licht worden gekanteld om de draagbalken onder het rack aan te kunnen brengen. Bij dit kantelen ging het vermoedelijk mis, want om 14:12[46] uur schakelde de primaire node[47] SERVER03[48] over naar de secundaire node SERVER01 die zich in de andere MER bevond (in het vervolg wordt deze actie de '*failover*' genoemd).

De storagenode gaf om 14:12:05 de melding '*Power fault encountered*'. Deze gebeurtenis vormde de oorzaak van de failover. Tijdens de werkzaamheden is er geen spanningsuitval geweest en zijn er ook geen kabels losgeraakt. Wel werd later duidelijk dat het moederboard van de storagecontroller defect was geraakt. Op basis van de melding in de logging is niet met zekerheid te zeggen dat de vijzelwerkzaamheden het incident veroorzaakt hebben, maar het in tijd samenvallen van het incident en de voorbereidende werkzaamheden voor het vijzelen van het rack, maken dit wel zeer aannemelijk. Vanaf het moment dat de storage overschakelde naar de andere server, draaide de volledige storage op de controller van SERVER01. De medewerkers van het ziekenhuis merkten niets van de failover. Functioneel draaide het systeem gewoon door.

Op het moment dat de failover plaatsvond, was een storagespecialist voor migratiewerkzaamheden aanwezig in het ziekenhuis.[49] Hij ontving een automatisch gegenereerde email van de failover. De specialist nam vervolgens contact op met de systeembeheerders, waarbij bleek dat zij nog geen actie hadden ondernomen op de failover. Eén van de systeembeheerders meldde daarna aan de projectgroep per WhatsApp dat storagenode SERVER03 down was en dat de storagespecialist onderweg was om te controleren wat er mis was gegaan. De storagespecialist nam op zijn beurt contact op met de *systeembeheerder storage* van het ziekenhuis te Purmerend (het voormalige Waterland ziekenhuis). Dit was zijn directe collega, die verantwoordelijk was voor de storage in beide ziekenhuizen. Deze *systeembeheerder storage* raadpleegde de analysetools van de fabrikant van de storage (*On Command System Manager*) en kwam tot de conclusie dat de communicatie tussen de beide controllers (van SERVER01 en SERVER03) was uitgevallen. Gewapend met deze informatie ging de storagespecialist naar de MER om te controleren of alle bekabeling nog verbonden was. Bij een visuele inspectie van deze bekabeling trof hij geen losse kabels aan, noch bleken er kabels te ontbreken.

46 Splunk logfile analyse.
47 Met node wordt in dit verband de helft van een storagecluster bedoeld. Zo'n cluster bestaat uit twee identieke servers (controller met opslagmedia) die elkaar overnemen bij hardware falen van één van deze servers.
48 SERVER01 en SERVER03 zijn de geanonimiseerde benamingen van de storageservers in respectievelijk MER2 en MER1.
49 Het Dijklander ziekenhuis, dat vanaf 7 januari 2019 bestaat, is voortgekomen uit een fusie tussen het Westfriesgasthuis en het Waterland ziekenhuis. Tijdens de ICT-storing in 2018 waren de ICT-afdelingen van beide ziekenhuizen nog niet samengevoegd. Medewerkers die verantwoordelijk waren voor de samenvoeging van de netwerken, werden op basis van hun specifieke kennis af en toe ingezet voor migratiewerkzaamheden bij het Westfriesgasthuis.



Figuur D8 Tijdlijn aanvang werkzaamheden tot uitval storagenode.

De storagespecialist vond de belasting van de resterende controller wel aan de hoge kant. Om performanceproblemen voor te zijn, besloot hij om 15:56 uur om een terugschakeling naar node SERVER03 te forceren met een forced takeback[50]. Dit resulteerde vrij kort daarna (enkele minuten) in een totale uitval van de storageserver (SERVER03). Na het uitvallen van de storageserver raadpleegde de storagespecialist van het ziekenhuis per abuis de (nieuwe) onderhoudspartij van de nieuwe storageserver. Hoewel de defecte storageserver niet door deze partij werd onderhouden, besloten zij toch om de storagespecialist telefonisch aanwijzingen te geven om checks op het systeem uit te voeren. Uit deze checks bleek dat de controller van SERVER03 defect was.

Om circa 17:00 uur kwam de *systeembeheerder storage* ter plaatse. Hij besloot een forced takeback te geven om zo de storage weer terug te schakelen naar de nog steeds werkende node in de andere MER. Dit commando herstelde de storagenode, maar vanwege de lange downtime moesten alle van de storage gebruikmakende servers in de juiste volgorde herstart worden. Dit proces duurde tot circa 20:45 uur, waarna het ICT-systeem weer beperkt beschikbaar was.[51] Parallel hieraan werd om circa 17:15 uur een prio-1 melding bij de juiste onderhoudspartij aangemaakt voor de storing.[52] Na deze melding trachtte de onderhoudspartij vergeefs toegang te krijgen tot het systeem om een analyse te kunnen doen. Uiteindelijk gaf de fabrikant van het systeem, via derdelijns support, op afstand instructies om via de seriële interface[53] van het systeem door de storagespecialist commando's te laten geven. Uit de responses van de storageserver op deze commando's kwam naar voren dat het moederboard van de controller defect was. Het was op dat moment circa 23:10 uur.[54]

50 Een commando waarmee de storage geforceerd wordt overgeschakeld van de ene node naar de andere node.
51 Logboek ICT.
52 Retrospectieve analyse ICT-storing 16-17 juli 2018.
53 De seriële interface van apparatuur is een interface op de apparatuur zelf waar direct een beheerlaptop op kan worden aangesloten. Deze interface wordt over het algemeen gebruikt wanneer beheer op afstand (om wat voor reden dan ook) niet meer mogelijk is.
54 Eindrapportage WFG, 25 oktober 2018.

Om 02:41 uur werd een vervangend moederboard bij het ziekenhuis afgeleverd. Om 03:59 uur[55] was ook het personeel van de onderhoudspartij aanwezig en kon worden begonnen met het omwisselen van de defecte controller. Dit vervangen duurde circa vier uur. Enerzijds omdat het systeem niet up-to-date bleek te zijn, anderzijds omdat de monteur niet bekend was met het vervangen van controllers en ervoor gekozen heeft om de reparatie zorgvuldig uit te voeren (met telefonische ondersteuning van de leverancier). Voordat de onderhoudspartij begon met omwisselen, werd daarom eerst gecontroleerd of de ontbrekende updates wel of niet noodzakelijk waren. Na lang heen en weer bellen met de leverancier van het systeem, bleek de vervanging van hardware ook te kunnen worden gedaan zonder dat het systeem up-to-date zou zijn. Daarnaast moest eerst de rommelige bekabeling van het systeem op orde worden gebracht en gelabeld. Rond 11:45 uur was het systeem weer volledig operationeel en na synchronisatie van alle systemen was om 13:30 uur de storing ten einde.

D.3.2 Analyse toedracht

Voorbereiding op de werkzaamheden

In de voorbereiding op de werkzaamheden is een PRI opgesteld. Een PRI is volgens de praktijkgids van het VMS veiligheidsprogramma bedoeld om voor risicovolle processen de risico's gestructureerd inzichtelijk te maken en voor de grootste risico's zoveel mogelijk mitigerende maatregelen te nemen. Een PRI is in opzet meer bedoeld voor processen die regulier worden uitgevoerd, maar kan (zoals hier het geval is) ook uitstekend worden gebruikt voor een eenmalig proces.

Voor de PRI werd de HFMEA[56] of BowTie methodiek gebruikt. De invulling hiervan door het Dijklander Ziekenhuis was als volgt: bij een PRI inventariseert een multidisciplinaire groep deskundigen in één bijeenkomst van maximaal vier uur de grootste risico's. De groep gaat na welke processtappen het meest risicovol zijn, welke faalwijzen kunnen optreden en hoe ernstig dat is. Wat zijn de oorzaken en hoe vaak leiden deze tot ongewenste gevolgen? Vervolgens worden beheersmaatregelen opgesteld om het optreden van het risico zoveel mogelijk te vermijden of de gevolgen van het optreden van een risico te beperken.

Het gekozen proces was de scope van de bouwkundige werkzaamheden die in de technische ruimte moesten plaatsvinden. Dit proces werd conform de richtlijn opgesplitst in deelprocessen (bestellen materialen, montage koelinstallatie, etc.). Per deelproces zijn de risico's van de bijbehorende werkzaamheden ingeschat. Het multidisciplinaire team bestond uit vijf inhoudsdeskundigen (vloerleverancier, monteur elektrische installatie, adviseur ICT-beheer, technische dienst en de *Chief Information Security Officer* (CISO)) en voldeed hiermee aan de richtlijnen uit de praktijkgids. Ook inhoudelijk waren voor de werkzaamheden de juiste disciplines vertegenwoordigd. Wel kan worden opgemerkt dat er niemand was om de risico's voor de zorg in te schatten.

De geïdentificeerde risico's richtten zich vooral op de risico's dat de werkzaamheden niet konden worden afgerond en veel minder op de eventuele gevolgen voor de patiënt of

55 Logboek ICT.
56 Healthcare Failure Mode Effect Analysis.

de patiëntveiligheid. In de uitwerking van de PRI is het risico op het uitvallen van apparatuur in de MER geïdentificeerd als een risico met een grote impact en de gevolgen van het kantelen van de kasten zouden een extreme impact hebben op de geleverde zorg. Tijdens de PRI is onder andere gesproken over de gevolgen van het niet-beschikbaar hebben van het patiëntendossier, wat maakte dat dit risico direct als "extreem" is geduid. De in de PRI opgevoerde mitigerende maatregel richtte zich echter alleen op het controleren van de bekabeling en niet op de gevolgen van een eventuele uitval van apparatuur. Hiermee werd een substantieel risico van de werkzaamheden: uitval van apparatuur en daarmee uitval van voor de patiënt belangrijke systemen, onvoldoende afgedekt met maatregelen. Opvallend is dat dit risico maar heel beperkt was uitgewerkt in beheersmaatregelen. Niet alle apparatuur die zich in de technische ruimte bevond was even kritisch. Het risico had verder uitgewerkt kunnen worden door te inventariseren welke apparatuur bij falen het grootste risico voor de continuïteit van het zorgproces zou geven. Specifiek voor deze risicovolle apparatuur hadden aanvullende mitigerende maatregelen kunnen worden genomen.

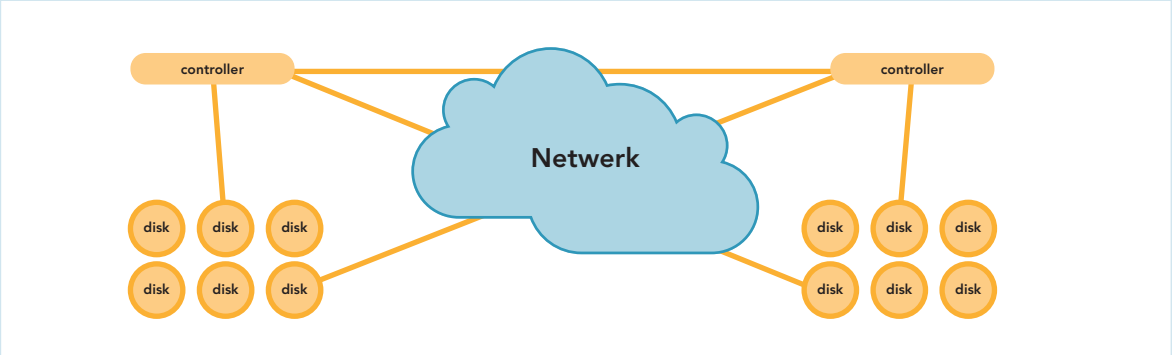
Uitvoering van de werkzaamheden
Over het tijdstip van de uitvoering van de werkzaamheden adviseerde de CISO om de werkzaamheden op vrijdag na 17:00 uur te starten en dan in het weekend te voltooien. Hier werd uiteindelijk geen gehoor aan gegeven.[57] Besloten werd, op aangeven van de directie van het Dijklander Ziekenhuis, om de werkzaamheden in ieder geval pas na 16:00 uur te starten. Dit omdat dan de meeste operatiekamers klaar zouden zijn en de poliklinieken hun werkzaamheden afronden. De belangrijkste reden om de werkzaamheden niet naar de avond en/of het weekend te verplaatsen, waren de kosten die uitvoering van de werkzaamheden buiten kantoortijden met zich meebrachten.

De voorbereidende werkzaamheden startten om 12:30 uur, nadat om 12:00 uur de kick-off was gehouden. Bij deze voorbereidende werkzaamheden was geen ICT-personeel aanwezig in de MER. De werkzaamheden bestonden uit het ter plaatse brengen van de benodigde materialen, maar ook uit het bevestigen van het vijzelmaterieel aan de apparatuur racks. Vooral die laatste activiteit was risicovol voor de aanwezige ICT-apparatuur. Zowel het aanbrengen van draagbalken in een werkend apparatuur rack als het aanbrengen van een draagbalk onder een werkend apparatuur rack zijn risicovolle handelingen. Men voerde immers zeer dicht in de buurt van de werkende apparatuur werkzaamheden uit. Uitschietend gereedschap kan direct tot een verstoring leiden.

D.3.3 Analyse techniek
Het ziekenhuis maakte gebruik van een storageserver waarop alle benodigde data voor programma's van gebruikers op een centrale plek werden opgeslagen. In dit geval was deze storageserver vormgegeven door een zogenaamd, *Metrocluster,*[58] zonder back-up faciliteit. Een Metrocluster bestaat uit twee identieke storagesystemen, die ieder weer zijn opgebouwd uit drie componenten: de opslagmedia (disks), de controller en het netwerk. De opslagmedia worden gebruikt voor de daadwerkelijke opslag van data;

57 Retrospective analyse ICT-storing 16-17 juli 2018.
58 Dit is een leverancierspecifieke type-aanduiding van een (storage)cluster.

het netwerk om de beide clusterdelen met elkaar te verbinden en de controller om de data-uitwisseling met de gebruikers van de storage te regelen.



Figuur D9 Schematische weergave storage.

De opslagmedia bestonden uit een aantal (reeksen van) opslagdisks. De opslagdisks waren zo ingericht dat bij het defect raken van een disk deze kon worden vervangen door een andere, zonder dat de inhoud van de defecte disk verloren zou gaan. Daarnaast waren de clusters ook gespiegeld ten opzichte van elkaar. Ze waren volledig identiek ingericht, zodat bij uitval van een volledig cluster (alle disks en controller aan één zijde), het andere cluster de werkzaamheden volledig zou kunnen overnemen. In een normale situatie hebben beide controllers controle over hun 'eigen' deel van de disks. Zodra een controller faalt, schakelt de controle van het gefaalde systeem automatisch over naar de secundaire controller. Doordat hier echter geforceerd werd teruggeschakeld naar een defecte controller, kon één zijde van het storagesysteem toch geheel uitvallen. Bij het geforceerd terugschakelen worden allerlei checks die het systeem zelf doet gepasseerd, zelfs als dit verlies van functionaliteit betekent.

De veerkracht van het storagesysteem was groot. Alle componenten (controller, netwerk en disks) konden falen zonder dat het systeem zijn functie zou verliezen. Dit falen gaat in principe zonder onderbreking. Dit bleek ook in de praktijk goed te werken: zodra de controller als gevolg van de werkzaamheden faalde, schakelde het systeem automatisch over naar node SERVER01.[59] Dit overschakelen werd niet door de gebruikers opgemerkt.

De structuur van het systeem betreft vooral de inrichting van het systeem. Het systeem was, vanuit de basis niet op een gestructureerde manier opgebouwd, maar organisch gegroeid. Een gevolg hiervan was bijvoorbeeld dat bepaalde data niet op disks staat met de juiste performancekarakteristieken. Dit had op haar beurt weer een effect op de belasting van de controllers Zo'n suboptimale inrichting kan als effect hebben dat de performance van het systeem bij een failover sterk terugloopt. Eerder (februari 2018) was een voorval opgetreden wat dit nog verder illustreert: inzet van een verkeerd type disks voor een bepaalde taak zorgde voor substantiële performanceproblemen bij de gebruikers van de storage. Bij het onderzochte incident heeft het ontbreken van structuur geen rol van betekenis gehad. Aannemelijk is dat de storagespecialist de belastingproblemen van het systeem ernstiger heeft ingeschat dan dat deze werkelijk waren (zie ook de volgende paragraaf onder de kop *Incident management*).

59 Splunk logfile analyse.

De schaalbaarheid van het systeem was bij aanschaf van het systeem voldoende om de behoefte van het ziekenhuis destijds (2013) in te vullen.[60] Gezien de aanschafdatum 2013[61] was het systeem wel aan het einde van zijn levenscyclus.[62] Het Dijklander Ziekenhuis had daarom al een nieuw systeem aangeschaft en de migratie van data naar het nieuwe systeem werd al gerealiseerd. De schaalbaarheid van het bestaande systeem was met het oog op deze vervanging minder van belang.

D.3.4 Analyse beheer

Voor de uitval van de storage in het Dijklander Ziekenhuis, zijn de volgende beheerprocessen van belang:

- Event management
- Incident management
- Service Level management
- Release management
- Capacity management
- IT service continuity management.
- Change management

Bij de keuze van de analyse van processen is vooral gelet op de directe oorzaken en de afhandeling van het incident. De beoordeling geschiedt op basis van wat waargenomen is in de analyse van het incident.

Event management

De failover van de storageserver werd opgemerkt door een systeembeheerder via automatische monitoring van het systeem. De storagespecialist kreeg ook een melding van het systeem en heeft in overleg met de systeembeheerder besloten om ter plaatse te gaan kijken. Onbekend is of de systeembeheerder op dat moment een incident heeft aangemaakt. Duidelijk is wel dat het event management proces gefunctioneerd heeft. De failover van de storageserver werd opgemerkt en er werd actie ondernomen.

Incident management

Een failover van de storageserver is in potentie een urgent incident. Immers een groot deel van de ICT-diensten die aan het ziekenhuis wordt geleverd, is afhankelijk van een correct werkende storage. De failover van de storage betekende in dit geval dat één van de twee controllers defect was. Dit betekende een aanzienlijk risico voor functieverlies op de ICT-diensten van een groot aantal gebruikers. Daarmee was er reden genoeg dit incident hiërarchisch te escaleren. Dit is niet gebeurd. De manager ICT werd zich pas bewust van de storing toen het ziekenhuis verlies van belangrijke functionaliteit opmerkte (om ca. 16:00 uur[63]). Het systeem draaide op dat moment gedurende een krappe twee uur op een enkele controller, wat een risicovolle situatie was.

60 Splunk logfile analyse.
61 Support contract Metrocluster leverancier, 20 juni 2013 en interviews Dijklander Ziekenhuis.
62 De gemiddelde levensduur van ICT-apparatuur in de zakelijke omgeving is circa 5 jaar. Dit hangt samen met de ondersteuning van de apparatuur door de leverancier en de voortschrijdende technische ontwikkelingen die nieuwe features biedt die niet meer mogelijk zijn met de bestaande apparatuur. Na deze 5 jaar is het gebruikelijk om nieuwe hardware aan te schaffen en eventuele migratie van bestaande naar nieuwe hardware in gang te zetten.
63 Retrospectieve analyse ICT-storing 16-17 juli 2018 en interviews Dijklander Ziekenhuis.

De initiële analyse van het incident zoals deze werd uitgevoerd door de storagespecialist was correct. In overleg met de *systeembeheerder storage* werd vastgesteld wat de symptomen van het probleem waren (verstoorde communicatie tussen de beide controllers) en welke checks het beste konden worden uitgevoerd (controle van de bekabeling). De storagespecialist voerde de nodige checks op het systeem uit, maar kon buiten een hoge belasting van het systeem geen anomalieën vinden. Hij besloot daarom terug te schakelen door het geven van het commando forced takeback. Dit commando leidde ertoe dat enkele ogenblikken later de gehele storageserver SERVER03 uitviel. Dit commando werd zonder verder overleg gegeven. Het systeem gaf tijdens het uitvoeren van het commando waarschuwingen voor verlies van data, hetgeen de storagespecialist kennelijk heeft genegeerd.

De vraag die zich opdringt is waarom de storagespecialist zich genoodzaakt voelde om het forced takeback commando uit te voeren. Er zijn twee factoren aan te wijzen die de storagespecialist heeft meegewogen bij dit besluit. De storagespecialist gaf allereerst aan dat het systeem een hoge belasting had. De CPU-load[64] van het systeem bleek ongeveer 85% te zijn tegen 35% onder normale operatie.[65] Bij een CPU-load van 95% en hoger zijn er performanceproblemen te verwachten. De load van 85% was daarmee binnen de marges van de normale performance van het systeem. Deze conclusie wordt onderschreven door het feit dat er geen meldingen uit het ziekenhuis zijn gekomen tijdens de failover periode (14:12 uur – 15:57 uur) over een lage performance van het systeem. Het tweede dat meespeelde was dat de inrichting van het systeem sinds de installatie niet gestructureerd is bijgehouden of geoptimaliseerd, maar min of meer organisch is gegroeid. Dat de inrichting van het systeem hiaten vertoonde, blijkt ook uit een eerder incident met de storageserver in februari 2018, waarbij een gebruik van een niet geschikt type disk voor bepaalde activiteiten zorgde voor substantiële performance-problemen op de storageserver.

Service Level management
Het Dijklander Ziekenhuis had een 'gold' level beheercontract bij de onderhoudspartij. Dit betekent dat de onderhoudspartij in geval van hard- en softwarestoringen het eerste aanspreekpunt is voor technische ondersteuning. Voor hardware heeft de onderhoudspartij de ondersteuning op haar beurt doorgecontracteerd naar de fabrikant van de storageapparatuur. Er zijn daarbij alleen garanties afgesproken voor het aannemen van de melding en voor het beschikbaar hebben van een technicus voor ondersteuning. Het oplossen van de storing of het leveren van hardware gebeurt zonder gegarandeerde oplostijd (best effort). Dit betekent dat het Dijklander Ziekenhuis zelf verantwoordelijk was voor de invulling van het eerste- en tweedelijns onderhoud en de onderhoudspartij het derdelijns onderhoud en de levering van reserveonderdelen voor zijn rekening zou nemen. Aangezien er in het contract met de onderhoudspartij geen voorraad reserveonderdelen is opgenomen, was het een logische optie dat het Dijklander Ziekenhuis zelf een reservevoorraad aan zou houden om de gewenste beschikbaarheid van de storage te kunnen garanderen. Dit bleek echter niet het geval. Er was geen reservevoorraad in het Dijklander Ziekenhuis aanwezig en daarmee was de

64 Dit is de belasting van de Centrale Processor Unit. Dit wordt meestal uitgedrukt in een percentage van de maximale belasting.
65 Logging storageserver SERVER01

beschikbaarheid van het systeem afhankelijk van het best effort contract met de onderhoudspartij.

Het systeem was verouderd en was na het verlopen van het initiële supportcontract (drie jaar na aanschaf van het systeem medio 2013) verlengd, maar de software werd daarmee niet meer automatisch bijgewerkt. Uit het supportcontract van de onderhoudspartij blijkt dat de installatie van technische software en firmware updates los staan van de normale werkzaamheden en apart worden gefactureerd. Aangezien de storageserver end-of-life was en het Dijklander Ziekenhuis al circa 1,5 jaar aan het migreren was naar een nieuw systeem, is het systeem sinds deze migratieperiode niet meer bijgewerkt met software-updates.

Uit het onderzoek komt verder naar voren dat de operationele afspraken over de rolverdeling tussen de onderhoudspartij, de fabrikant en het Dijklander Ziekenhuis niet zijn opgenomen in een *Dossier Afspraken en Procedures*. Dit betekent dat de operationele afspraken met betrekking tot beheer tussen de onderhoudspartij en de fabrikant enerzijds en de ICT-afdeling van Dijklander Ziekenhuis anderzijds niet helder waren, maar ad-hoc werden ingevuld bij een storing.

Het geheel van gemaakte afspraken met onderhoudspartijen en eigen beheeractiviteiten van het ziekenhuis was onvoldoende om een kritisch systeem als de centrale storage voldoende gegarandeerd beschikbaar te houden. Zaken als ontbrekende reserveonderdelen, niet gestructureerde configuraties en niet bijgewerkte software-updates vormen een direct risico op de beschikbaarheid van het systeem.

Release management
Het niet goed up-to-date houden van het systeem, zoals hierboven is geconstateerd, duidt op een omissie in release management. Bij dit incident zorgde dit voor een vertraging in de installatie van de vervangende controller. Eerst moest gecontroleerd worden of dit wel mogelijk was in een systeem waarvan de software niet was bijgewerkt. Daarmee ging kostbare tijd verloren.

Capacity management
De inschattingsfout van de storagespecialist over de ernst van de performanceproblemen van het systeem, als ook de eerdere performanceverstoring als gevolg van foutieve diskinzet, duiden op omissies in capacity management. Capacity management is er juist op gericht om tijdig te signaleren dat er zich knelpunten manifesteren zodat hier ook tijdig maatregelen voor kunnen worden genomen. Dat voorkomt situaties waarbij ad-hoc beslissingen noodzakelijk zijn. Het is beter om ad-hoc beslissingen in een risicovolle situatie te mijden, omdat de kans op fouten dan hoger is.

IT service continuity management
IT service continuity management richt zich op de uitzonderlijke situatie dat normale maatregelen gefaald hebben en continuïteit van bedrijfskritische processen geraakt wordt. Bij dit incident was daar sprake van toen de storageserver SERVER03 uitviel. Dit is een uitzonderlijke situatie, omdat voor deze uitval minimaal een dubbele fout moet optreden.

Een maatregel die de gevolgen van de uitval van de storageserver had kunnen mitigeren, was de beschikbaarheid van een nood-EPD. Het EPD was in dit geval het bedrijfskritische systeem. Dit systeem kwam in de BIV-kwalificatie op de hoogste score uit (beschikbaarheid hoog, integriteit hoog en vertrouwelijkheid hoog). Het nood-EPD bestaat uit een aparte applicatie, waarop een kopie van het EPD kan worden geraadpleegd. Deze kopie loopt maximaal 15 minuten achter op het reguliere EPD. De kopie kan alleen geraadpleegd worden en wijzigingen moeten op papier bijgehouden worden. Tijdens de uitval van de storageserver bleek het nood-EPD echter niet inzetbaar, omdat voor de toegang tot dit nood-EPD van dezelfde (defecte) storageserver gebruik werd gemaakt. Op basis van een correcte invulling van IT service continuity management en de naleving ervan had deze afhankelijkheid er niet mogen zijn.

Change management
Als het incident wordt beschouwd, dan valt op dat de wijzigingen in de MER (het verhogen van de vloer), niet als een ICT-change waren aangemerkt. Daardoor was ook onbekend op welk moment welke systemen verhoogd zouden worden en was er ook geen gerichte voorbereiding op storingen als gevolg van de werkzaamheden.

Samenvattende conclusie
De storing in het Dijklander Ziekenhuis was een direct gevolg van werkzaamheden in de MER van het ziekenhuis. Ondanks dat de werkzaamheden in deze MER uitgebreid waren voorbereid door middel van een PRI waren de ICT-risico's in deze PRI onvoldoende inzichtelijk gemaakt. Voor de ICT-risico's die wel benoemd waren, zijn onvoldoende mitigerende maatregelen genomen.

De voorbereidende werkzaamheden werden niet als risicovol ingeschat, maar bleken dit wel te zijn. Dit heeft ertoe geleid dat met deze risicovolle werkzaamheden is gestart op een moment dat het ziekenhuis in vol bedrijf was.

De failover van de storage als gevolg van de voorbereidende werkzaamheden had onmiddellijk tot verhoogde waakzaamheid moeten leiden. Dit is echter niet gebeurd: de failover werd niet geëscaleerd naar hoger management en ook de gecontracteerde onderhoudspartij werd niet geraadpleegd of gewaarschuwd.

De combinatie van binnen de ICT-afdeling belegde operationele beheerwerkzaamheden en bij de leverancier/fabrikant gecontracteerd onderhoud, maakte het onmogelijk om garanties af te geven op beschikbaarheid van de storagefunctionaliteit. Gezien het belang van de storage voor het primaire proces van het ziekenhuis zouden deze garanties er wel moeten zijn.