Bijlage F
Beschrijving andere incidenten

Den Haag, februari 2020

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

BESCHRIJVING ANDERE INCIDENTEN

Deze bijlage bevat een beschrijving van drie ICT-storingen die in 2018 en begin 2019 hebben plaatsgevonden in het Amsterdam UMC (locatie VUmc), het Medisch Spectrum Twente en de Noordwest Ziekenhuisgroep. De Onderzoeksraad heeft deze bijlage opgesteld op basis van het onderzoek dat de ziekenhuizen en hun ingehuurde ICT-dienstverleners zelf hebben uitgevoerd. De Onderzoeksraad heeft geen onderzoek gedaan naar deze incidenten en kan dus ook niet beoordelen of de bevindingen en analyses van andere partijen correct zijn. Het feit dat de Onderzoeksraad de bestaande documenten heeft gebruikt om een weergave te kunnen geven van de incidenten, betekent dus niet dat de Onderzoeksraad de bevindingen en conclusies uit die documenten onderschrijft. Daarvoor is eigen onderzoek nodig.

De incidenten worden in het rapport opgenomen om te laten zien dat de drie door de Onderzoeksraad onderzochte incidenten niet op zichzelf staan. Dat de Onderzoeksraad geen onderzoek heeft gedaan naar deze incidenten, wil niet zeggen dat er uit deze voorvallen geen lessen te trekken zijn. Het is de verantwoordelijkheid van de ziekenhuizen om de incidenten te evalueren en verbeterpunten te formuleren. De Onderzoeksraad hoopt daar met dit rapport een bijdrage aan te kunnen leveren.

LIJST VAN AFKORTINGEN

BHV	Bedrijfshulpverlening
BNO	Bedrijfsnoodorganisatie
CBT	Crisisbeleidsteam
CIO	Chief Information Officer
EPD	Electronisch patiëntendossier
ICT	Informatie- en communicatietechnologie
ISO	Information Security Officer
MST	Medisch Spectrum Twente
MOS	Medisch Oproepsysteem
NWZ	Noordwest Ziekenhuisgroep
SEH	Spoedeisende Hulp
SLA	Service Level Agreement
SMB	Server Message Block
SVM	Storage Virtual Machine
VOS	Verpleegkundig Oproepsysteem

LIJST VAN BEGRIPPEN

Aggregatieswitch
Switch die verkeer van eindapparatuur verzamelt en bundelt.

Bugfix
Verbetering van een (software) fout.

Clusternodes
Computers die onderdeel uitmaken van een cluster.

Coreswitch
Switch die de samengevoegde (geaggregeerde) datastromen in een netwerk behandelt.

Domaincontroller
Een domaincontroller is een centraal in het netwerk opgestelde server die op basis van authenticatie gebruikers toegang geeft op centrale diensten (zoals filetoegang, toegang tot printers etc.).

Electieve operaties
Operaties waar iemand bewust voor kiest (in tegenstelling tot noodzakelijke- of spoedoperaties).

Extender
Apart toegangsplatform om daarmee de poortcapaciteit van een aggregatieswitch te verhogen.

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

File-lock
Het administratief reserveren van filetoegang voor een gebruiker.

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 beschikbaar is.

Low level logging
Het vastleggen van gedetailleerde logberichten van een apparaat.

Netwerkswitch
Zie switch.

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

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

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.

Storagenode
Het samenstel van opslagmedia en controller.

Storage Virtual Machine
Een storagenode die als software entiteit op een gedeeld hardwareplatform draait.

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

Unidirectional link
Communicatie over een verbinding in een netwerk is niet meer in twee richtingen mogelijk, maar slechts in één richting.

BIJLAGE F

F.1 ICT-storing Amsterdam UMC, locatie VUmc

F.1.1 Inleiding

Op maandag 22 oktober 2018 kwamen om circa 08:00 uur in de ochtend de eerste meldingen binnen bij de ICT-afdeling van het Amsterdam UMC, locatie VUmc met betrekking tot de traagheid van de standaardwerkomgeving genaamd 'View'.[1] Het aantal meldingen aan de Servicedesk nam dusdanig toe dat om 09:15 uur werd besloten het ICT-crisisteam op te starten. De symptomen van de storing waren het niet beschikbaar zijn van de M- en N-schijf en traagheid binnen de standaardwerkomgeving. Personeel dat was ingelogd op deze werkomgeving kon blijven werken, maar het ontbreken van de N-schijf zorgde ervoor dat nieuwe pogingen om in te loggen niet slaagden. Gedurende de dag werd een aantal mogelijke oorzaken onderzocht (netwerk, storage[2], werkomgeving (view), domaincontrollers[3]), maar er kon geen duidelijke oorzaak worden gevonden. Omdat de domaincontrollers al langere tijd een hoge belasting lieten zien, werd besloten om extra domaincontrollers bij te plaatsen. De situatie leek echter alleen maar te verslechteren. Om 17:25 uur werd een eigenaardigheid in de koppeling tussen netwerk en storage opgemerkt. Of dit de oorzaak van de storing was bleef onduidelijk, maar de koppeling was in ieder geval niet correct. Besloten werd om hier een correctie op toe te passen. Het was op dat moment inmiddels 21:00 uur. Vanwege het tijdstip op de dag was het veel rustiger op het systeem en leek alles zich stabiel te gedragen.

Op dinsdag 23 oktober 2018 om 08:00 uur werd bij de eerste bijeenkomst van het crisisteam duidelijk dat hetzelfde probleem zich nog steeds manifesteerde. Het werd ook duidelijk dat het verbinden van de N-schijf (storageserver SERVER01[4]) met een ander netwerk het probleem oploste en dat er daarna wel kon worden ingelogd op View. De bedrijfsnoodorganisatie (BNO) besloot tot het sluiten van poliklinieken, de spoedeisende hulp (SEH) en de shockrooms.[5] Later die dag (15:30 uur) is besloten om, vanwege de

1 Major incident rapportage ICT verstoring, v0.8.
2 De storage zijn alle systemen die bedoeld zijn om digitale gegevens in op te slaan.
3 Een domaincontroller is een centraal in het netwerk opgestelde server die op basis van authenticatie gebruikers toegang geeft op centrale diensten (zoals filetoegang, toegang tot printers etc.).
4 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.
5 Logboek bijeenkomsten CT ICT storing 23 & 24 oktober, 2018.

onverwachte acute situatie (faillissement van het Slotervaart Ziekenhuis), de SEH weer te openen. Daarnaast werd besloten om een VIP-lijst te maken van gebruikers die nog mochten inloggen op het systeem.

Om 18:20 uur lagen er vier mogelijke oplossingen op tafel waarvan er twee realistisch genoeg waren om verder uit te werken. Deze oplossingen waren: 1) het ontkoppelen van persoonlijke data en systeemdata; 2) het ontsluiten van de N-schijf (storageserver SERVER01) op een ander (nieuw) netwerk. Het ontkoppelen van de persoonlijke data en de systeemdata (optie 1) was lastiger en tijdrovender dan optie 2 (ander netwerk). Omdat optie 2 goed leek te werken, koos men daarvoor. De werkzaamheden hiervoor waren om 20:45 uur gereed. Bij de start van het ziekenhuis op 24 oktober 2018 zouden conform de VIP-lijst steeds meer gebruikers in de nieuwe situatie (via het nieuwe netwerk) worden vrijgegeven om in te loggen. Buiten wat administratieve tegenslagen[6] bleek de aanpak goed te werken. De rest van de dag werden steeds meer gebruikers ontsloten op de nieuwe situatie en om 15:47 uur was de situatie zodanig genormaliseerd dat van het einde van de storing kon worden gesproken.[7]

F.1.2 Toedracht

Technische achtergrond bij het incident

De storing kent geen duidelijk oorzaak. In de analyse van het ziekenhuis wordt gewezen op een opeenstapeling van factoren die van invloed zijn geweest op de storing. Deze factoren zijn[8]:

- In de drie jaar voorafgaand aan de storing zijn er op de bij de storage betrokken netwerkswitches geen softwarepatches doorgevoerd. Ook heeft de apparatuur lange tijd geen herstart ondergaan.
- De apparatuur waar de storage aan gekoppeld is, is standaard niet ontworpen om datastromen uit dergelijke storagesystemen af te handelen. Bij zware belasting zal dataverlies zeker optreden en de performance sterk afnemen.
- Bij de analyse van low level logging[9] van de extenders[10] is aangetoond dat er abnormale omstandigheden waren ten tijde van de storing. Signaalniveaus vanuit de storageserver SERVER01 voldeden niet meer aan gestelde limieten. Poorten hebben zichzelf meerdere malen herstart, wat netwerkonderbrekingen veroorzaakte.
- In de maanden voorafgaand aan de storing waren er al meerdere storingen geweest die te relateren waren aan performanceproblemen op View in combinatie met de storageserver SERVER01. De oplossing lag toen in het uitbreiden van storageserver SERVER01 clusternodes[11]. Dit is een indicatie dat ook het gebruik van de storageserver SERVER01 voor N- en M-schijven alsmaar toenam en een verhoging van belasting op het Nexus netwerk bewerkstelligde.
- Uit een op dat moment recente health check op het storageserver SERVER01 platform, kwam het advies om de redundante koppeling met het netwerk aan te

6 Met administratieve tegenslagen wordt hier bijvoorbeeld bedoeld: gebruikers die niet op de VIP-lijst staan maar daar wel op behoren te staan of gebruikers die bepaalde rechten missen.
7 Major incident rapportage ICT verstoring, v0.8.
8 RootCauseAnalysis_traagheidView_Amsterdam UMC, locatie VUmc_V05
9 Low level logging is het vastleggen van gedetailleerde logberichten van een apparaat.
10 Een extender is een apart toegangsplatform om daarmee de poortcapaciteit van een aggregatieswitch te verhogen.
11 Clusternodes zijn computers die onderdeel uitmaken van een cluster.

passen naar een andere netwerk adaptermodus. Ondanks dat de modes[12] al jaren ook werd toegepast op een ander storagesysteem (M-schijven) dat ook gebaseerd is op Linux, zou de modes mee kunnen spelen in de performancedegradatie van de storageserver SERVER01 in combinatie met de bestaande netwerkomgeving.

Deze factoren in overweging nemende kan het volgende worden gesteld:

Het niet updaten van software kan betekenen dat bepaalde softwarefouten optreden die eigenlijk al opgelost zijn in een nieuwere versie van de software. Het lange tijd niet herstarten van de switches[13] kan (als gevolg van gebrekkig geheugengebruik) leiden tot geheugenproblemen, wat op zich weer tot onvoorspelbaar gedrag van de switch zou kunnen leiden.

De switch fabric extender kan worden beschouwd als een apart toegangsplatform om daarmee de poortcapaciteit van een aggregatieswitch[14] te verhogen. De standaardtoepassing voor deze apparatuur is een omgeving waar vele netwerkpoorten nodig zijn met per netwerkpoort een beperkte hoeveelheid data. Storagepoorten wijken sterk af van deze standaardtoepassing en genereren juist veel verkeer per poort. Zeker aangezien werd vermeld dat de storagenodes zijn uitgebreid als gevolg van performanceproblemen, is te verwachten dat de belasting van de switch fabric extender ook is toegenomen.

De analyse van de *switch fabric extender* brengt fouten naar boven die ten tijde van de storing optraden. Nadere analyse van de foutmeldingen die in de logs van de apparatuur voorkomen, vertonen sterke overeenkomst met de foutmeldingen beschreven in een bug report van de netwerkapparatuurleverancier. Dit report vermeldt een hardwarefout die ervoor zorgt dat de interface van de apparatuur op 1Gbps instelt in plaats van op 10Gbps. Dit zou verklaren waarom het systeem bij lage belasting wel functioneert. Niet te achterhalen is echter of de interface daadwerkelijk op 1Gbps was geconfigureerd.

F.1.3 Technische Incidentbestrijding

Maandag 22 oktober 2018

Nadat rond 08:00 uur de eerste meldingen werden gedaan over de traagheid van View en deze meldingen in aantal toenamen, werd om 09:15 uur besloten om het ICT-crisisteam te starten. Als eerste werden de gebruikers via het intranet geïnformeerd dat er problemen waren met de standaardwerkomgeving. De analyse werd gestart. Daar kwam in eerste instantie uit dat de (overschreden) capaciteit van de domaincontrollers mogelijk de oorzaak van de problemen was. Het bijplaatsen van extra domaincontrollers loste het incident echter niet op.[15] De symptomen verergerden juist. Rond 17:25 uur werd vastgesteld dat het redundant verbinden van de storage met het netwerk niet goed functioneerde. Hoe lang dit zo heeft gefunctioneerd is onbekend, maar besloten werd om deze foutieve, dubbele koppeling voorlopig om te zetten naar een enkele koppeling

12 Hiermee wordt een de instelling van het systeem bedoeld.
13 Een switch is een netwerkapparaat dat data kan schakelen op basis van een MAC-adres.
14 Een aggregatieswitch is een switch die verkeer van eindapparatuur verzamelt en bundelt.
15 Major incident rapportage ICT verstoring, v0.8.

om er in ieder geval zeker van te zijn dat dit niet de problemen veroorzaakte. Het was op dat moment 21:00 uur en deze oplossing leek een stabiele situatie te creëren.

Dinsdag 23 oktober 2018
De volgende dag manifesteerde zich rond 8:00 uur hetzelfde probleem. Besloten werd om de diverse leveranciers te betrekken bij het zoeken naar de oorzaak van de storing. Bij een test om de storage via een ander netwerk aan te sluiten, bleek dat dat wel een goede performance gaf. Omdat nog niet duidelijk was wat de oorzaak van de storing was en de storing gerelateerd leek aan de belasting van het systeem, werd besloten om alleen urgente gebruikers van het systeem toe te laten. Hiervoor werd een VIP-lijst opgesteld van afdelingen die vervolgens technisch werd geïmplementeerd, zodat alleen gebruikers van de VIP-lijst nog konden inloggen op het systeem. De resultaten van deze actie waren wisselend. Sommige VIP-afdelingen konden prima werken, anderen ondervonden nog steeds grote problemen. Rond 18:00 uur lagen er vier mogelijke opties op tafel. Daarvan was er één het meest eenvoudig uit te voeren, omdat daarvoor aan de inrichting van data niets hoefde te worden veranderd. Deze optie was om de storage te ontsluiten via het nieuwe netwerk. Het alternatief was een scenario waarbij van de N-schijf de persoonlijke data en de systeemdata zijn gescheiden. Toen bleek dat het inzetten van het alternatieve netwerk goede resultaten gaf, werd hiermee verder gegaan.

F.1.4 Technische analyse
Uit de technische analyse van het probleem komen vier opvallende punten naar voren.

Allereerst valt op dat pas in een relatief laat stadium is besloten om de externe leveranciers te betrekken. Deze werden ingeschakeld op dinsdag 23 oktober in de ochtend, toen bleek dat de eerder in gang gezette oplossing (het verbreken van de foutieve netwerkkoppeling) niet het gewenste resultaat liet zien.

Ten tweede valt op dat de betrokken leveranciers niet direct tot een duidelijke analyse of oplossing konden komen. Verwonderlijk is dat niet. Het ziekenhuis doet zelf het *eerste-* en *tweedelijns* onderhoud. Daarmee worden de leveranciers voor het *derdelijns* onderhoud ingezet. Zij hebben daarmee ook geen actueel beeld van de technische configuratie. Doordat de oorzaak van de storing niet duidelijk was (en ook later niet wordt), kan ook niet effectief aan een oplossing worden gewerkt. De gevonden problemen zijn wel anomalieën van het systeem, maar niet de oorzaken van de storing. Een voorbeeld daarvan is het geconstateerde probleem met de domaincontroller. Ook het activeren van een VIP-lijst blijkt de nodige haken en ogen te hebben. Het splitsen van data in de werkomgeving (N-schijf) is tijdrovend en blijkt uiteindelijk toch niet dé oplossing. Dit, gecombineerd met het gegeven dat de problemen pas echt optreden bij grootschalig gebruik van het systeem, maakt het zoeken naar de oorzaak niet eenvoudiger en daarmee tijdrovend.

Ten derde valt op dat achteraf geconcludeerd is dat de monitoring op de netwerkpoorten naar Fabric Extender (die op zijn beurt met de storage is verbonden), was uitgezet.[16] Dat maakte het lastig om vast te stellen wat er precies aan de hand was met die poorten. De

16 Health check Core 2018-Q4

Fabric Extender liet kennelijk wel duidelijke fouten zien, maar deze fouten worden niet vermeld in de rapportages van Amsterdam UMC (locatie VUmc) en zijn daarmee ook niet meegenomen in de analyse van de storing.

Een vierde en laatste punt dat opvalt, is dat de gebruikte switches vele bugfixes[17] achterlopen op de door de fabrikant vrijgegeven software. Ook is duidelijk dat de gecreëerde configuratie niet conform de best practices van de fabrikant is. Dit wekt de indruk dat de ICT-afdeling moeite heeft om het technische ontwerp, de inrichting en het beheer van het netwerk voldoende in te vullen. Belangrijk is om actueel zicht te houden op de gebruikte infrastructuur en eventueel daarin optredende fouten vroegtijdig te signaleren. Of deze activiteit nu bij de ICT-afdeling van het ziekenhuis wordt belegd of daarbuiten bij een leverancier of fabrikant is minder van belang, maar evident is dat er heldere afspraken moeten bestaan over hoe de taakverdeling is tussen partijen en wie waarvoor verantwoordelijk is. Dat maakt dat in geval van een storing veel sneller en gerichter kan worden gezocht naar een oorzaak, waardoor kostbare tijd wordt gewonnen.

F.1.5 Crisisbeheersing

Op maandag 22 oktober 2018 werd in de ochtend de omvang van de storing helder. Er was op dat moment echter geen eenduidig beeld. Degene die nog ingelogd waren, konden nog werken, maar ondervonden wel sterke vertraging. Medewerkers hadden geen toegang tot het merendeel van de systemen, waaronder het elektronisch patentendossier (EPD). Toegang tot het EPD was alleen nog mogelijk via bijzondere werkplekken.[18] Gedurende de dag werd een aantal mogelijke oorzaken gevonden en acties om deze te mitigeren in gang gezet. Uiteindelijk leek het oplossen van de fout in de koppeling tussen storage en netwerk de situatie te verbeteren. Het was op dat moment circa 23:00 uur en het besluit werd genomen om de volgende ochtend opnieuw de situatie op te nemen.[19]

Op dinsdag 23 oktober werd om 08:00 uur vastgesteld dat dezelfde problemen zich weer openbaarden. Dat was het signaal om de BNO op te starten. Besloten werd om alle relevante leveranciers te betrekken bij de storing. Ook werd besloten om de SEH en de ochtend polikliniek te sluiten. Aangezien de storing zich steeds duidelijker openbaarde naarmate het systeem zwaarder werd belast, werd er gewerkt aan een VIP-lijst van gebruikers. Doel hiervan was om de belasting van het systeem terug te brengen tot de strikt noodzakelijke gebruikers. Kort daarna (10:00 uur) werd besloten om de sluiting van SEH en poli's voort te zetten voor de rest van de dag. Uitzonderingen werden gemaakt voor acute poli-patiënten en de poli verloskunde. Operatiekamerprogramma's gingen wel door.

Vanaf 15:30 uur werd besloten de SEH voor acute zorg weer open te stellen. Dit in verband met de plotselinge sluiting van het Slotervaart Ziekenhuis. Op de afdelingen die wel doorwerkten, werd gebruik gemaakt van standalone PC's voor het EPD. Deze EPD-only werkplekken werden waar nodig aangevuld. Updates op het EPD werden op

17 Een bugfix is een verbetering van een (software) fout.
18 181029 Crisisevaluatierapportage ICT storing Amsterdam UMC, locatie VUmc (def. versie).
19 Major incident rapportage ICT verstoring, v0.8.

papier bijgehouden. De behandelaar zelf diende vast te stellen of deze werkwijze voldoende veilig was, in verband met het niet bijgewerkt zijn van het EPD. Vanaf ongeveer 13:00 uur werden via het Landelijk Crisis Management Systeem (LCMS) informatie updates aan de buitenwereld doorgegeven. Deze situatie bleef van kracht tot woensdag 24 oktober 15:47 uur, toen het einde van de storing formeel werd vastgesteld. Daarmee heeft het ziekenhuis een substantiële verstoring van het primaire proces (patiëntzorg) van circa 54 uur ondervonden. Van deze 54 uur werd 31 uur conform het Integraal Crisisplan gewerkt.

F.1.6 Analyse Crisisbeheersing

In het Integraal Crisisplan van het Amsterdam UMC (locatie VUmc) staan vijf categorieën van een crisis, oplopend van 'beperkt' tot 'catastrofaal'. Deze crisis is, gezien de uitval van interne processen, onduidelijke oorzaak en onduidelijke duur van de storing, geclassificeerd als een categorie 4 crisis (kritiek). In het zogenaamde motorkapoverleg[20] wordt bepaald of het bedrijfsnoodplan in werking wordt gesteld. Bij deze crisis gebeurde dat op 23 oktober om 08:00 uur.[21] De eerste signalen van de storing waren er echter al om 22 oktober om 09:15 uur.[22] Deze signalen waren toen zo ernstig dat besloten werd de ICT-crisisorganisatie te starten.

Uit de crisisevaluatierapportage blijkt dat er op 22 oktober 2018 meerdere malen vanuit de medisch en verpleegkundige coördinatie is verzocht om opschaling, echter dit verzoek is niet gehonoreerd. De argumentatie die voor deze beslissing is gegeven, is dat het lastig is om de impact van een storing in te schatten en dat de opschaling via de directeur medische zaken verloopt. In de crisisevaluatierapportage wordt geconcludeerd dat er eerder opgeschaald had moeten worden. Gezien de impact van de storing had dit in de loop van 22 oktober 2018 moeten plaatsvinden. De uitval van de ICT betekende bij deze crisis een sterke teruggang in de efficiëntie van het ziekenhuis en zette daarmee een rem op de capaciteit van het ziekenhuis. Het leveren van verantwoorde zorg aan nieuwe en aanwezige patiënten kwam hiermee onder druk te staan.

F.2 ICT-storing Noordwest Ziekenhuisgroep

F.2.1 Inleiding

Op 15 januari 2019 trad er om 23:45 uur een storing op in de storageomgeving van de Noordwest Ziekenhuisgroep (NWZ), een ziekenhuisorganisatie met locaties in Alkmaar, Den Helder, Heerhugowaard, Limmen, Schagen en Texel. Deze storing betekende voor de medewerkers van deze locaties dat zij geen toegang meer hadden tot het EPD. Het EPD zelf werkte nog wel, maar de snelkoppeling die door de gebruikers wordt gebruikt om het EPD te benaderen, was niet meer beschikbaar.[23] Gedurende de nacht zochten het ziekenhuis, de partij waar de storage aan is uitbesteed (de externe provider) en de

20 De term 'motorkapoverleg' kan in deze context verwarrend werken. Bedoeld is hier een intern telefonisch eerstelijns Amsterdam UMC, locatie VUmc overleg waarbij wordt bepaald of de dreigende calamiteit binnen de lijn wordt opgelost, of dat het nodig is om de BNO op te schalen.
21 181029 Crisisevaluatierapportage ICT storing Amsterdam UMC, locatie VUmc (def. versie).
22 Major incident rapportage ICT verstoring, v0.8.
23 Toedracht, 15 januari 2019 MW.20190119.1.

leverancier van de storageserver naar een oplossing, maar deze is niet gevonden. Om 07:15 uur werd de noodprocedure van het ziekenhuis opgestart. Geplande operaties en afspraken werden geschrapt. Dit betrof zowel de poliklinieken, medisch ondersteunende diensten (zoals radiologie en nucleaire geneeskunde) als het geplande operatiekamer programma (alle electieve geplande operaties). Semi-spoed-, spoedoperaties en oncologiebehandelingen werden nog wel uitgevoerd. De SEH was uitsluitend geopend voor instabiele patiënten.[24] Om 10:00 uur werd een workaround voor het probleem gevonden, die ervoor zorgde dat er weer toegang was tot het EPD. Deze workaround werd vrijgegeven (circa 10:45 uur) en korte tijd daarna (circa 11:30 uur) bleken meer dan 1.000 van de 3.000 medewerkers weer gebruik te maken van het EPD.[25]

Om 12:20 uur werd de daadwerkelijke oorzaak van de storing gevonden. De storing werd veroorzaakt door een activiteit van een managementserver van de externe provider. Deze server werd gedeactiveerd waarna de storage zich herstelde en de situatie voor het ziekenhuis normaliseerde.[26] Om 13:39 uur werd de storing afgemeld en om 14:00 uur werd de normale bedrijfsvoering van het ziekenhuis hervat.[27]

F.2.2 Toedracht

NWZ heeft de opslag van haar data uitbesteed aan een externe provider. Voor de opslag van de data wordt door de externe provider een storageserver gebruikt. Deze storageserver wordt door meer klanten van de externe provider gebruikt, zonder dat deze klanten bij elkaars data kunnen komen. NWZ heeft op deze storageserver (net als de andere klanten) zijn eigen Storage Virtual Machine[28] (SVM).

Gemeenschappelijk gebruik van hardware, software of diensten kan altijd leiden tot onbedoelde beïnvloeding van de gebruikers onderling. Wanneer de hardware van een gedeelde server defect raakt, zullen alle gebruikers hier het effect van merken. Dit is niet anders dan bij een falen van de hardware van een server die slechts door één gebruiker wordt gebruikt. Minder duidelijk ligt het bij een falen van de door alle gebruikers gebruikte software. Hierbij kan een actie van een gebruiker leiden tot een fout die ook een effect heeft op de andere gebruikers van het systeem. De storing bij NWZ is een voorbeeld van een dergelijke situatie. Nog minder duidelijk is dat bij een storing het gecontracteerde onderhoud (maintenance) ook een gedeelde capaciteit is. Op het moment dat er veel storingen tegelijk optreden of dat er een zeer lastige en hoge prioriteit storing optreedt bij één gebruiker, zullen de andere gebruikers dit merken in hun responsetijden. Dit is de niet-vermijdbare keerzijde van gedeeld gebruik van hard- of softwarediensten.

24 Evaluatie Interne Crisisorganisatie uitval ICT, 15 januari 2019.
25 Technische analyse netwerkverstoring, 15 januari 2019.
26 Toedracht, 15 januari 2019 MW.20190119.1.
27 1e uitvraag IT storing en antwoorden, 7 februari 2019.
28 Een storagenode die als software entiteit op een gedeeld hardwareplatform draait.

De storing werd veroorzaakt door een limiet in het aantal file-locks[29] die de storageserver tegelijk kon aanhouden. Het maximale aantal simultane file-locks bleek rond de 400.000 te liggen en dit getal is een limiet voor alle gebruikers van de fysieke storage apparatuur; zelfs als deze gebruikers logisch van elkaar gescheiden zijn in SVM's. Het grote aantal file-locks werd veroorzaakt door een file-duplicatie van de beheerder van het systeem op één van hun eigen servers (geen NWZ server). Het vastzetten van files is een functionaliteit die is toegevoegd aan Network File System versie 4 (NFSv4). De eerdere versie NFSv3 kende deze functionaliteit niet. De storing werd uiteindelijk verholpen door de server van de externe provider uit te zetten. Hierdoor daalde het aantal file-locks onder de limiet en herstelde de functionaliteit voor NWZ. Als oplossing van de storing is teruggegaan naar NFSv3 en met de leverancier van de storage wordt bekeken of er op het aantal file-locks monitoring kan worden gerealiseerd, zodat er tijdig een waarschuwing kan worden gegeven.

Een file-lock is het administratief reserveren van filetoegang voor een gebruiker. Dit mechanisme wordt gebruikt om te voorkomen dat twee (of meer) gebruikers tegelijk dezelfde files gaan bewerken en als gevolg daarvan elkaars wijzigingen mogelijk ongedaan maken. In NFSv3 is dit als een apart protocol (Network Lock Manager) gerealiseerd. In NFSv4 is het reserveren (locken) van files een integraal onderdeel van het NFS-protocol geworden. Het blijkt echter dat deze functionaliteit in NFSv4 een capaciteitsbeslag op de storage hardware legt en er daarmee een limiet ontstaat voor het aantal simultane open files.

F.2.3 Technische Incidentbestrijding

Op 14 januari kwam om 23:45 uur de melding binnen bij de afdeling ICT dat het EPD niet beschikbaar was. Het eerste vermoeden van de ICT-medewerkers van het ziekenhuis was dat het probleem de toegangsrechten op het systeem betrof, waardoor het EPD niet kon worden benaderd. ICT-medewerkers van het ziekenhuis namen telefonisch contact op met de nieuwe hostingleverancier voor alle servers, en met de toenmalige hostingleverancier voor alle servers.[30]

Bij controle van de logfiles van de storage werd een melding gevonden die wees op een probleem met de storageserver en niet met de toegangsrechten, zoals eerder werd gedacht. Om 04:13 uur werd er daarom een prio-1 melding bij de leverancier van de storage aangemaakt.[31] Om 04:00 uur werd ook een interne opschaling gedaan naar de CIO en IT-Operations manager van de NWZ.[32] Om 06:00 uur is geforceerd een failover[33] uitgevoerd naar een andere controller[34] van dezelfde storageserver. Opvallend is dat na deze actie het systeem voor ongeveer vijf minuten herstelde, waarna dezelfde foutmelding verscheen en het systeem weer onbruikbaar werd. Daarom werd besloten

29 Een file-lock is het administratief reserveren van filetoegang voor een gebruiker.
30 Storingsverslag van een IT-consultancy firma.
31 Service Incident Report long form van fabrikant.
32 Verslag evaluatie storing Noordwest Ziekenhuisgroep, 15 januari 2019.
33 De overschakeling van de primaire node naar de secundaire node.
34 De controller regelt het schrijven van en naar de disks van de storageserver.

om om 06:30 uur, 10:00 uur en 11:32 uur nogmaals een geforceerde failover uit te voeren en daarbij het netwerkverkeer te monitoren. Dit bleek geen duidelijke aanwijzing te geven waar de fout zich bevond. Een mogelijk verdachte server van NWZ is uitgezet, maar dat verhielp het probleem niet.

De suggestie is gedaan om het Server Message Block (SMB-) verkeer vanuit het ziekenhuis geheel te blokkeren. SMB-verkeer is het netwerkprotocol dat gebruikt wordt om in Microsoft Windows bestandsuitwisseling tussen meerdere computers mogelijk te maken. Het blokkeren van het SMB-verkeer stond de ICT-afdeling van het ziekenhuis niet toe. De gevolgen van een dergelijke blokkade zouden te ingrijpend zijn voor het primaire proces van het ziekenhuis.[35]

Tot dan toe werden de logs gefilterd op verkeer van het ziekenhuis. Toen werd besloten om de logs ongefilterd (dus voor alle klanten op de diverse SVM's) uit te voeren, werd er een server gevonden die waarschijnlijk het probleem veroorzaakte. Uit deze nieuwe logs bleek echter dat niet SMB het probleem veroorzaakte, maar Network File System (NFS). Dat is een vergelijkbaar protocol voor bestandsuitwisseling als SMB, maar dan de Linux[36] variant. Om 12:28 uur werd de nieuw gevonden server uitgezet. Dit loste het probleem op en vanaf dat moment herstelde de storage zich voor het ziekenhuis.

F.2.4 Crisisbeheersing

De dienstdoende crisiscoördinatoren ontvingen tussen 23:45 uur en 01:00 uur de melding van het incident. Om 04:00 uur is als gevolg van de voortdurende storing opgeschaald naar het ICT-management van NWZ en het management van de betrokken partijen.[37] Conform de noodprocedure van uitval van het EPD zijn in de loop van de nacht op aanvraag noodlaptops uitgereikt om patiëntinformatie na te lezen. Ook is overgegaan op papieren registratie. Voor de communicatie met de buitenwereld is het LCMS ingezet. Rond 05:30 uur besloten de crisiscoördinator en een lid van de raad van bestuur tot opschaling en is een gezamenlijk Crisisbeleidsteam (CBT) en Operationeel Beleidsteam gepland. Hierbij is in eerste instantie ingezet op fase 2 (kritiek), achteraf wordt vastgesteld dat fase 3 (catastrofaal) wellicht meer van toepassing was. Dit omdat de reikwijdte van de storing het gehele ziekenhuis trof.[38] Om 07:15 uur is de noodprocedure geactiveerd[39] en kwamen in een eerste gezamenlijke vergadering het CBT, het Operationeel Beleidsteam en het Facilitair Crisisteam bij elkaar. In het CBT nam de manager ICT plaats als deskundige. In het overleg is besloten om de poli's te sluiten, de SEH te sluiten (met uitzondering van de instabiele patiënten) en operatiekamerprogramma's te schrappen.[40] Als gevolg van de besluiten werden 75 electieve[41] operaties uitgesteld en 200 polibezoeken geannuleerd. Tot de storing onder

35 Storingsverslag van een IT-consultancy firma.
36 Linux is een besturingssysteem. Een besturingssysteem is een set van programma´s die het opstarten en de basisfuncties van een computer faciliteert. Programma´s maken daarna gebruik van deze besturingssoftware om de hardware aan te sturen. Voorbeelden van veelvoorkomende besturingssystemen zijn Microsoft Windows, Apple macOS, Linux, Apple iOS en Android.
37 Technische analyse netwerk verstoring, 15 januari 2019.
38 Evaluatie interne crisisorganisatie bij uitval ICT, 15 januari 2019.
39 Storingsverslag van externe provider.
40 Evaluatie interne crisisorganisatie bij uitval ICT, 15 januari 2019.
41 Electieve operaties zijn operaties waar iemand bewust voor kiest in tegenstelling tot noodzakelijke- of spoedoperaties.

controle was (ca 13:30 uur), kwamen deze crisisteams individueel nog vijf maal bijeen. Het geheel werd om 15:00 uur met een gezamenlijke bijeenkomst afgesloten.

F.2.5 Analyse technische incidentbestrijding en crisisbeheersing

Om circa 03:00 uur werd duidelijk dat het ging om een verstoring van de storageserver waardoor de gebruikersprofielen niet werden geladen.[42] Het EPD kende geen verstoring (want dat draait op een andere omgeving)[43], maar door het niet laden van de gebruikersprofielen is de toegang tot het EPD niet mogelijk. Het is opvallend dat deze informatie al om 03:00 uur beschikbaar was, maar dat het zoeken naar een workaround pas veel later begon (rond 06:00 uur).[44] De workaround was vervolgens spoedig gevonden en bleek ook goed te werken.

De storing zelf bleek te worden veroorzaakt door een technische limiet in de storageoplossing. Dat deze technische limiet werd bereikt, was een gevolg van een server van een externe partij en valt daarmee buiten het beheer van het ziekenhuis. Het ziekenhuis had hier verder ook geen kennis van. In de afgesproken Service Level Agreement (SLA)[45] met de externe partij staat dat een prio-1 melding binnen 2 uur hersteld moet zijn. Deze limiet is in dit geval niet gehaald, want het incident had conform die norm om 03:00 uur opgelost moeten zijn. Daarmee kan de conclusie worden getrokken dat de NWZ wel afdoende afspraken had gemaakt met de externe partij, maar dat dit geen garantie biedt dat ook daadwerkelijk ieder prio-1 incident binnen de afgesproken norm wordt afgehandeld.

In de technische afhandeling van de storing komt een aantal elementen naar boven die vertragend werken in de oplossing van het probleem, of die de communicatie over de oplossing compliceren. Zo bleek het service managementtool van de fabrikant niet beschikbaar te zijn. Hierdoor kon het incident niet automatisch in het hoogste storingsniveau worden geplaatst waardoor geautomatiseerde processen voor de storingsafhandeling niet startten.[46] Verder bleek een complicerende factor dat het hier een uitbestede storageomgeving betrof. Voor de technische afhandeling van het incident was daarmee niet het ziekenhuis het primaire aanspreekpunt, maar de storage service provider. Dit zorgde ervoor dat het ziekenhuis de technische communicatie over de storing uit tweede hand kreeg en dat escalatie richting de fabrikant ook indirect ging.

Feitelijk was direct vanaf de start van het incident (23:45 uur) duidelijk dat dit bij voortduring zou leiden tot opschaling van de crisisorganisatie. Bij de verdere escalatie naar CIO-niveau rond 04:00 uur en het creëren van de prio-1 melding was duidelijk dat dit een kritisch incident was (fase 2 crisisbeleid) dat het normale bedrijfsproces van het gehele ziekenhuis trof. Om 06:00 uur besloten de crisiscoördinator en een lid van de raad van bestuur om op te schalen naar CBT niveau. Het CBT kwam om 07:15 uur voor

42 Verslag evaluatie storing Noordwest Ziekenhuisgroep, 15 januari 2019.
43 Overzicht Relevante Apparatuurleveranciers.
44 Technische analyse netwerk verstoring, 15 januari 2019.
45 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.
46 Verslag evaluatie storing Noordwest Ziekenhuisgroep, 15 januari 2019.

het eerst bij elkaar. Op dat moment was, blijkens de evaluatie van de crisisbeheersing, de voorbereiding op het operatieprogramma zonder patiëntstromen al gestart (om 06:45 uur).

F.3 ICT-storing Medisch Spectrum Twente

F.3.1 Inleiding

Op 11 januari 2019 om even na 06:00 uur merkte een servicedeskmedewerker van het Medisch Spectrum Twente (MST) dat geen van zijn systemen te bereiken waren. De medewerker belde met de Bedrijfshulpverlening (BHV) om hier melding van te maken. Kort hierna bleek er ook een telefoniestoring te zijn.

Al snel werd duidelijk dat de situatie ernstig was. Men wist niet hoe lang de storing zou gaan duren. Daarom werd besloten om alle spoedpatiënten om te leiden naar andereziekenhuizen en de noodprocedures in gang te zetten. Alle patiënten met een ochtendafspraak op de polikliniek werd gevraagd om niet naar het ziekenhuis te komen. De operatiekamers, SEH en alle poliklinieken werden preventief gesloten. Er zijn geen patiënten overgeplaatst die al in het ziekenhuis waren ten gevolge van de storing.
Ondertussen was de externe ICT-dienstverlener op de hoogte gesteld van de storing en gevraagd om ondersteuning. Op basis van meldingen uit het systeem dat het netwerk monitort en een eigen analyse van de storing, vermoedde de externe ICT-dienstverlener dat het probleem zich in een coreswitch[47] bevond. De coreswitch bevond zich echter in een apparatuurkast waarvan de sloten via het netwerk worden bediend. De netwerkstoring maakte dat dit niet meer kon, waarna besloten werd de kast met een koevoet te openen.

Verder kwam men erachter dat de nieuwe noodprocedure niet direct gebruikt kon worden door het ontbreken van de juiste instellingen op de tablets waar men mee werkte. Doordat de telefooncentrale niet werkte en de medewerkers van de externe ICT-dienstverlener niet beschikten over mobiele telefoonnummers, van bijvoorbeeld de dienstdoende escalatiemanager, hadden ze moeite om te communiceren met verschillende mensen in het ziekenhuis. Als extra complicerende factor bleek de ontvangst van het mobiele netwerk in het datacenter zeer slecht te zijn. Er was een noodcentrale voorzien die geheel los van het gewone netwerk stond, maar in de ontstane situatie werd het inschakelen van deze centrale geheel over het hoofd gezien (dit stond ook niet in de noodprocedures).

Nadat de coreswitches herstart waren, werden ook de overige switches herstart waarna het netwerk zich herstelde en weer beschikbaar kwam. Het systeem voor verplegers om opgeroepen of gealarmeerd te worden (VOS/MOS[48]) bleek echter nog niet te werken. Het ziekenhuis meldde de storing hiervan bij de externe leverancier en meldde dat het ging om “prio-1”. Op het moment dat na een uur nog geen reactie was ontvangen, nam het ziekenhuis opnieuw contact op met hen om te benadrukken dat het om een hoge

47 Een *coreswitch* is een *switch* die de samengevoegde (geagregeerde) datastromen in een netwerk behandeld.
48 Deze afkortingen staan voor respectievelijk het Verpleegkundig Oproepsysteem en het Medisch Oproepsysteem.

prioriteit ging. Hierop liet deze leverancier het ziekenhuis weten dat zij een afspraak met het ziekenhuis hebben dat zij een reactietijd mogen hanteren van vier uur (conform *Service Level Agreement* (SLA)[49]). Uiteindelijk was ongeveer drie uur na de melding een medewerker van de leverancier ter plaatse om de storing op te lossen. Dit was binnen de tijd zoals afgesproken in de SLA. Desondanks heeft de verpleging hinder ondervonden van het niet werken van het systeem.

Het ziekenhuis kon na een storing van ongeveer twaalf uur weer over tot de normale bedrijfsvoering. Gedurende de storing waren de ICT-applicaties niet beschikbaar voor het personeel. Er was ook geen telefonie of wifi beschikbaar. Het bedrijfsnoodplan werd in werking gesteld. Er moesten papieren medicatielijsten handmatig worden verstrekt, poliklinische afspraken voor vrijdagochtend werden grotendeels geannuleerd of verzet en de SEH moest worden gesloten. 27 operaties gingen die dag niet door en zestien patiënten zijn naar andere ziekenhuizen doorverwezen. Het ziekenhuis geeft aan dat de patiëntveiligheid niet in het geding is geweest.

F.3.2 Toedracht

Tijdens en na de storing heeft de ICT-dienstverlener getracht vast te stellen wat de oorzaak is geweest en is een root cause analyse[50] geschreven. Daarin staan bevindingen en conclusies over de toedracht van de storing. In deze analyse beschrijft de ICT-dienstverlener dat er een storing is geweest op een belangrijk knooppunt in het netwerk.[51] Gedacht werd aan twee mogelijke oorzaken van de storing.

Hardware probleem

Een mogelijke oorzaak die de ICT-dienstverlener aanwijst voor de storing is een probleem met een defecte glasvezelkabel of *interface*. Aan deze oorzaak werd gedacht, omdat in de logbestanden van een switch, waar de storing zich in voordeed, staat dat er sprake is geweest van een "*unindirectional link*".[52] Dat betekent dat er een probleem is tussen twee netwerkapparaten (switches). Hieronder staat uitgelegd hoe een dergelijk probleem ontstaat.

49 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.

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

51 Datacenter netwerk core.

52 Jan 11 05:51:57.392: %UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface Gi1/0/2, unidirectional link detected.

Alle communicatie over een netwerk is tweerichtingsverkeer. Een verbinding tussen A en B functioneert correct wanneer zowel verkeer van A naar B als van B naar A mogelijk is. In netwerken wordt vaak gebruik gemaakt van optische signalen die door glasvezels worden gestuurd. In het geval van optische transmissie zijn er twee aparte glasvezels, één voor zenden en één voor ontvangen.[53] Er bestaat daarmee een kans dat of de zender of de ontvanger defect raakt. In dat geval is er nog communicatie mogelijk, maar slechts in één richting. Dit wordt een unindirectional link genoemd.

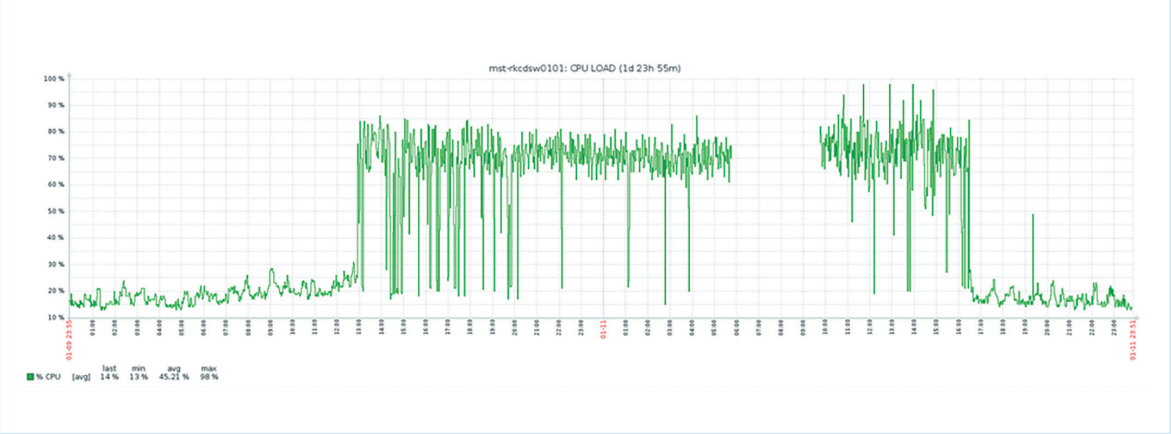
Binnen dit netwerk was een protocol actief (Spanning Tree Protocol[54]) dat voorkomt dat er loops[55] in het netwerk ontstaan. De aanwezigheid van een unindirectional link in het netwerk kan ervoor zorgen dat het Spanning Tree Protocol een onderbreking tussen twee locaties vaststelt. Gevolg hiervan kan zijn dat alsnog een loop in het netwerk ontstaat waardoor het netwerk vastloopt.

Om het ontstaan van unindirectional links te voorkomen is het mogelijk om unindirectional link detection in het netwerk aan te zetten. In het geval van een unindirectional link schakelt de switch dan automatisch de nog wel werkende link uit, waarmee een loop in het netwerk wordt voorkomen. In het geval van MST was unindirectional link detection actief. De ICT-dienstverlener vermoedt dat de loop al was ontstaan voordat unindirectional link detection ingreep. Hoe en waar de unindirectional link door is ontstaan is niet vastgesteld.

Verkeerde configuratie laptops
Een andere mogelijkheid die de ICT-dienstverlener heeft onderzocht is dat een of meerdere laptops met twee netwerkkaarten voor overbelasting op het netwerk hebben gezorgd. Zo zag de ICT-dienstverlener de dag voor de storing een verhoogde belasting op het netwerk van de twee coreswitches. De ICT-dienstverlener had een grens ingesteld wanneer de monitoringsoftware, die activiteit op het netwerk in de gaten houdt, een waarschuwingsmelding moet geven. De verhoogde activiteit bleef daar echter net iets onder, waardoor de ICT-dienstverlener geen waarschuwing kreeg. De dienstverlener gaf aan dat dit wel vaker is voorgekomen. Maar nog niet eerder duurde de hoge belasting van de switch zo lang en was de belasting zo hoog.

Onderstaande grafiek komt uit de monitoringssoftware van de ICT-dienstverlener die kijkt naar de belasting van de switch. Te zien is dat de grafiek scherp omhoog schiet. Als de switch uitgeschakeld staat, is de grafiek onderbroken. Pas enige tijd nadat de switch weer is ingeschakeld, daalt de grafiek weer.

53 Dit kan ook op één enkele vezel worden gecombineerd waarbij zenden en ontvangen op dezelfde vezel gebeurd. Voor de hier beschreven problematiek is dit niet relevant.
54 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.
55 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 beschikbaar is. Dit fenomeen staat uitvoerig beschreven in bijlage D.2 (IJsselland Ziekenhuis).



Figuur F1: Monitorgegevens belasting switch.

Op de maandag na het incident zag men opnieuw deze verhoogde belasting. Men zag dat vanuit een bepaald deel van het netwerk de belasting ontstond en sloot dit deel vervolgens af. Hierop daalde de belasting van het netwerk weer. Men herleidde de zware belasting naar twee laptops die verkeerd geconfigureerd zijn door de gebruiker(s). Deze verkeerde configuratie zou ervoor hebben gezorgd dat twee wifi netwerken van het ziekenhuis (die voor gasten en personeel) gekoppeld werden aan "externe netwerken". Hierdoor ontstond overbelasting, doordat oneigenlijk verkeer op het netwerk van het ziekenhuis terecht kwam.

F.3.3 Technische incidentbestrijding

Om 06:07 uur meldde een BHV-medewerker van MST telefonisch via de servicedesk van de ICT-dienstverlener dat er sprake was van een storing waardoor "niets meer werkt" (intranet, email en applicaties).[56] De ICT-dienstverlener analyseerde vervolgens de logfiles van netwerkapparatuur. Dit bleek lastig, omdat sommige switches door de storing de centrale logserver niet konden bereiken. Ook had een aantal switches niet de juiste tijdsinstellingen ingesteld staan door een onbekend en vermoedelijk ongerelateerd probleem. Dat zorgde er echter voor dat het lastiger was om te zien op welk tijdstip er wat is gebeurd.[57] De ICT-dienstverlener signaleerde na de eerste technische analyse dat er specialisten op locatie moesten komen, maar dit kostte tijd.[58] Op het moment dat de ICT-dienstverlener de dienstdoende escalatiemanager probeerde te bellen, bleek dit niet mogelijk, omdat ook de telefooncentrale in storing was.

Om de switches opnieuw op te starten, moest men de kasten waar de switches zich bevonden, openen. Dat lukte niet omdat de sloten op de kasten via het netwerk met elkaar verbonden waren en het netwerk in storing was. Tevergeefs probeerde de ICT-dienstverlener de kasten open te maken door de stroom van de sloten te halen en een wandplaat los te maken. Uiteindelijk zijn de kasten na één uur en drie kwartier door het gebouwbeheer van MST, na overleg tussen de ICT-dienstverlener en MST, opengebroken.

56 RCA MST Infrastructure Down, v1.0.
57 RCA Appendix, v0.3.
58 Rapportage ICT verstoring, 11 januari 2019.

Hierna besloten de ICT-dienstverlener en MST dat de urgentie van de storing zodanig was dat er geen tijd meer kon worden besteed aan de analyse van het probleem en dat de coreswitches, die zich in de opengebroken kasten bevonden, moesten worden herstart.[59] [60] Nadat deze waren herstart, kwamen geleidelijk de ICT-diensten weer beschikbaar. De applicaties die noodzakelijk waren voor de bedrijfsvoering werden getest en vervolgens vrijgegeven. Door synchronisatieproblemen duurde het tot omstreeks 12:00 uur 's middags totdat medewerkers de 1400 werkplekken weer in gebruik konden nemen. Er werd toen echter gesignaleerd dat het VOS/MOS-systeem niet werkte, omdat de coreswitches elkaar niet konden bereiken. Om dit op te lossen deed MST een prio-1 melding bij een andere ICT-dienstverlener. Uiteindelijk was om 15:30 uur een technicus van de ICT-dienstverlener bij het ziekenhuis aanwezig om de coreswitches te herbouwen. Omstreeks 17:30 uur is ook de storing van het VOS/MOS-systeem verholpen.

De daaropvolgende zaterdag en zondag deden zich verder geen bijzonderheden voor. Maar op maandag om 16:59 uur kreeg men een automatische melding vanuit het monitoring systeem dat er verdacht verkeer op het netwerk was en dan specifiek in het MST-Gast en MST-Personeel netwerk. Na een analyse van de ICT-dienstverlener bleek dat het verkeer ongebruikelijk was en mogelijk weer een storing kon veroorzaken. Daarom probeerde men het te stoppen door de dubbele uitvoering van deze netwerken terug te brengen naar een enkele uitvoering.

Op dinsdag kwam er een netwerkspecialist van de ICT-dienstverlener ter plaatse om het netwerk te analyseren. Deze achterhaalde twee laptops die het verdachte verkeer veroorzaakten. Deze laptops zijn vervolgens opgehaald en overgedragen aan de Information Security Officer (ISO).

Op woensdag bleek uit onderzoek dat op één van de laptops een tweede netwerkkaart geïnstalleerd was. Als deze verkeerd geconfigureerd wordt, kan dit een lus op het netwerk veroorzaken. Daardoor kan overbelasting ontstaan en het netwerk storing geven. Er werd extra apparatuur geplaatst om het netwerk te kunnen analyseren, maar er werd geen verdacht verkeer meer gevonden.

Ten slotte richtte men zich vanaf donderdag op de oorzaak van de storing. De uitkomsten daarvan zijn de Raad tot op heden onbekend.[61]

F.3.4 Crisisbeheersing

Het crisisteam kwam om 09:20 uur voor het eerst bijeen nadat om 06:15 uur in de ochtend de storing was gemeld aan de dienstdoende manager. Op het moment dat het crisisteam bijeenkwam, was vastgesteld dat het netwerk was uitgevallen en de telefoons niet werkten. Alle spoedpatiënten werden toen al omgeleid naar andere ziekenhuizen en de noodprocedure DSV was uitgerold. Ook waren de operatiekamers en de SEH gesloten voor de ochtend.

59 RCA MST Infrastructure Down, v1.0.
60 Rapportage ICT verstoring, 11 januari 2019.
61 Rapportage ICT verstoring, 11 januari 2019.

In de eerste bijeenkomst van het crisisteam werd besloten om patiënten in de hal te melden dat er een stroomstoring was, dat daardoor de patiëntendossiers niet toegankelijk waren en de poli's in de ochtend gesloten zouden zijn. Patiënten die toch naar de poli zouden komen, zouden weggestuurd worden met een nieuwe afspraak. Patiënten die geopereerd moesten worden, werden naar de balie verwezen voor meer informatie. Om welke informatie dat ging, is niet bekend. Via sociale media en lokale media besloot men naar buiten te brengen dat er sprake was van een ICT-storing. Men wilde daarbij benadrukken dat de patiëntveiligheid niet in gevaar was, maar dat het om preventieve sluitingen ging. Tenslotte besloot men de raad van toezicht te informeren.

Toen men om 11:00 uur opnieuw bijeenkwam, had het crisisteam het beeld dat de storing grotendeels voorbij was. Ze verwachtten op dat moment dat het nog ongeveer een uur zou duren voordat alles weer zou werken. Tevens dachten ze dat het VOS/MOS-systeem operationeel was. Het bleek echter ook dat veel huisartsen niets van de storing wisten en patiënten bleven doorsturen naar het ziekenhuis. MST was vervolgens voornemens de huisartsen te bellen om hen te informeren, omdat de telefonie weer werkte. Dit bleek achteraf niet goed te zijn gegaan. De operatiekamers en SEH bleven gesloten, totdat de ICT-problemen volledig waren opgelost. Sommige mensen die toch naar de poli waren gekomen, werden geholpen.

Om 12:00 uur bleek dat het VOS/MOS-systeem nog problemen gaf. Ook een andere applicatie die was vrijgegeven, bleek toch nog problemen te geven. De afdeling Radiologie bleek applicaties in gebruik te hebben genomen die nog niet waren vrijgegeven en huisartsen waren nog altijd niet voldoende van de storing op de hoogte. Men besloot dat er door het crisisbeleidsteam een lijst met knelpunten moest worden opgesteld ter evaluatie.

Om 14:00 uur bleek het VOS/MOS-systeem nog altijd niet te werken. De rest van de systemen was weer operationeel. Door de problemen met het VOS/MOS-systeem was verpleegkundig personeel opgeschaald en was de BHV aanwezig in de kliniek om te helpen. De operatiekamers waren weer geopend en men verwachtte achttien patiënten te kunnen helpen in de middag. Ook de SEH was weer open. Er waren nog wel problemen met monitoren op de SEH en een planbord wat noodzakelijk is voor regie op patiëntenlogistiek. Besloten werd dat de volgende dag pas zou worden afgeschaald op het gebied van ICT en dat er een klein crisisteam beschikbaar moest blijven voor eventuele nieuwe problemen die zich zouden kunnen voordoen.

Bij de laatste bijeenkomst van het crisisteam om 16:30 uur, was het VOS/MOS-systeem, nog niet werkzaam en was onbekend wanneer het opgelost zou zijn. De monitoren op de SEH konden geen verbinding met het netwerk maken, waardoor monitoring op afstand niet mogelijk was. Ook bleken er problemen met laboratoriumuitslagen die niet binnenkwamen, vanwege een probleem met versturen. Uitslagen werden daarom doorgebeld of gefaxt. De problemen met het planbord waren opgelost. Tot 23:00 uur was er extra personeel beschikbaar vanwege de problemen met het VOS/MOS-systeem.

F.4 Observaties bij deze incidenten

Bij de drie in deze bijlage beschreven incidenten komen verschillende factoren terug, die ook bij de drie meer diepgaand onderzochte voorvallen een rol hebben gespeeld.

Dit betreft met name onvolkomenheden in het ICT-beheer, zoals het uitvoeren van software-updates en de borging van de continuïteit van de (ICT-)dienstverlening. Ook blijkt bij meerdere incidenten de monitoring van systemen een aandachtspunt, vooral omdat het kan helpen bij het vaststellen van de oorzaak van een incident. Dit is een belangrijke voorwaarde om van een incident te kunnen leren. Het vaststellen van de oorzaak is bijvoorbeeld bij het incident in het Amsterdam UMC (locatie VUmc) voor zover bekend bij de Onderzoeksraad niet gelukt. Ook de afstemming tussen het ziekenhuis en de externe partijen speelt een rol bij de incidenten in deze bijlage, met name bij de technische incidentbestrijding in het Amsterdam UMC (locatie VUmc), het oplossen van het probleem met het VOS/MOS-systeem in het MST en het ontstaan van de storing in de NWZ. Bij de NWZ werd de storing namelijk veroorzaakt door een storing bij de externe provider van de storage.

Ook geven de in deze bijlage beschreven incidenten inzicht in tekortkomingen in de voorbereiding op ICT-incidenten. Dit wordt vooral goed geïllustreerd door het incident in het MST, waarbij tijdens het incident bleek dat de sloten van de apparatuurkasten afhankelijk waren gemaakt van het netwerk en men over het hoofd zag dat er een noodcentrale was. Het oefenen met een scenario van ICT-uitval kan juist dit soort onvoorziene problemen aan het licht brengen.

Tot slot blijkt uit de in deze bijlage beschreven incidenten dat een ICT-storing, net als bij de drie onderzochte ziekenhuizen, direct impact kan hebben op de patiëntveiligheid maar dat dit niet in alle gevallen direct wordt herkend. Dit leidde in het geval van de storing in het Amsterdam UMC (locatie VUmc) tot het niet-tijdig opschalen van de crisisorganisatie. Daarnaast besteden de ziekenhuizen die in deze bijlage centraal staan, in hun evaluaties van de incidenten nauwelijks tot geen zichtbare aandacht aan de impact van de ICT-uitval op de patiëntveiligheid. Niet in termen van letsel, noch in termen van verhoogde kans op schade voor de patiënt als gevolg van de storingen.