KPN – STORING
WAALHAVEN ROTTERDAM

- DEFINITIEF -

mei 2012

INHOUD

VOORWOORD

Telecommunicatievoorzieningen zijn van vitaal belang voor de samenleving. Mensen en organisaties zijn in de loop der tijd steeds afhankelijker geworden van deze voorzieningen. De storing in het telecomknooppunt in de Waalhaven te Rotterdam in juli 2011 bleef dan ook niet zonder gevolgen voor het maatschappelijk leven. Cruciale verbindingen van de hulpdiensten vielen voor een deel uit en diverse vitale organisaties ondervonden in meer of mindere mate hinder van het incident.

Telecommunicatievoorzieningen zijn kwetsbaar. Netwerken kunnen uitvallen door technische of natuurlijke oorzaken, maar ook kunnen menselijke fouten, criminaliteit of aanslagen hieraan ten grondslag liggen. Veel rampenplannen houden hiermee onvoldoende rekening en lijken ervan uit te gaan dat 'het allemaal wel goed zit' met telecommunicatie. Men verwacht dat de voorzieningen operationeel blijven en dat eventuele uitval veelal kan worden opgevangen met alternatieve diensten of voorzieningen. Toch is de afhankelijkheid groter dan men doorgaans beseft. Deze onbewuste afhankelijkheid, ook wel 'telekwetsbaarheid' genoemd, kan leiden tot maatschappelijke ontwrichting, onder andere door problemen in het functioneren van vitale organisaties.

Voor Agentschap Telecom en de Inspectie Veiligheid en Justitie (Inspectie VenJ) is het incident in Rotterdam aanleiding direct een onderzoek in te stellen, niet alleen naar de oorzaak en de aanpak van de storing, maar ook naar de maatschappelijk gevolgen van het incident. In welke mate was de openbare veiligheid in het geding en konden de organisaties die van cruciaal belang zijn voor de veiligheid nog naar behoren functioneren? Ook komt in het onderzoek aan de orde welke activiteiten zijn ondernomen om de mogelijke negatieve effecten zoveel mogelijk te elimineren.

Minstens zo belangrijk is de vraag hoe het zit met de voorbereiding. Hoe heeft KPN de risicobeheersing georganiseerd en op welke manier hebben zij hierover met de afnemers gecommuniceerd? En hoe zit het met de afnemers zelf? Zijn zij zich bewust van hun afhankelijkheden en kwetsbaarheden en op welke manier hebben zij zich voorbereid op mogelijke uitval?

In dit rapport zijn de antwoorden op deze en andere vragen opgenomen. Het onderzoek laat zien dat zowel KPN als de veiligheidsregio's en de andere vitale organisaties voortvarend hebben gereageerd op de storing en snel de juiste maatregelen hebben getroffen. Punten van kritiek liggen vooral op het terrein van de voorbereiding. In een aantal opzichten kan de risicobeheersing bij KPN transparanter en ook de communicatie met de afnemers moet worden verbeterd.

Agentschap Telecom en de Inspectie VenJ hebben het onderzoek gezamenlijk uitgevoerd. De belangrijkste overweging voor de samenwerking was te komen tot een bundeling van expertise en ervaring op het gebied van de telecommunicatie enerzijds en openbare orde en veiligheid anderzijds. Bovendien kon op die manier efficiënter worden gewerkt, ook naar de betrokken organisaties toe. Dit rapport is het resultaat van deze samenwerking.

Medio april 2012 was opnieuw sprake van storingen in het telecommunicatienetwerk. In dit geval betrof het (gedeeltelijke) uitval van het 112–netwerk. De Inspectie VenJ en Agentschap Telecom hebben besloten ook naar deze incidenten een onderzoek in stellen. In de zomer van 2012 wordt verslag gedaan van dit onderzoek.

Agentschap Telecom en de Inspectie VenJ beogen met de bevindingen, opmerkingen en aanbevelingen in dit rapport een bijdrage te leveren aan een veiliger Nederland, met name waar het gaat om de continuïteit van (vitale) telecommunicatie voor een vlot en veilig verloop van de maatschappelijke processen voor burgers, bedrijfsleven en overheid.

J.G. Bos

hoofd van de Inspectie Veiligheid en Justitie

P.A. Spijkerman

directeur-hoofdinspecteur van Agentschap Telecom

SAMENVATTING

1 Inleiding

Aanleiding

In de nacht van 26 op 27 juli 2011 pleegt KPN onderhoud aan het telecomknooppunt in de Waalhaven te Rotterdam. Tijdens dit onderhoud treedt een technische storing op in een zogenaamde 'cross connect'. Een cross connect is een belangrijk knooppunt in het netwerk van KPN. Het gevolg is dat 86 C2000-verbindingen en ongeveer 6200 andere transmissieverbindingen[1], vooral in gebruik voor telefonie en vaste dataverbindingen, gedurende bijna zeven uren worden verstoord.

Het uitvallen van de verbindingen heeft grote impact op de (vitale) infrastructuur binnen de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid, Hollands Midden en Zeeland. De storingen treffen onder meer verbindingen van en met banken, de verbinding tussen de meldkamer Zeeland en de ziekenhuizen, de luchtverkeersleiding van Rotterdam The Hague Airport, de metro in Rotterdam en de Rotterdamse haven. Ook automatische brandmelders en particuliere telefoonlijnen worden getroffen door uitval. De regio Zuid-Holland Zuid wordt geconfronteerd met storingen in de bereikbaarheid van het alarmnummer 112.

Uit de eerste contacten met de veiligheidsregio Rotterdam-Rijnmond komt het beeld naar voren dat door de storing de veiligheid en de dienstverlening binnen de regio sterk negatief is beïnvloed. Het functioneren van onderdelen van de vitale infrastructuur is daarbij in het geding geweest. Het hoofd van de Inspectie VenJ besluit hierop een onderzoek in te stellen naar de uitval, de gevolgen en de risico's die dit heeft gehad voor het functioneren van de hulpdiensten en andere (publieke) diensten. Omdat het uitvallen van (een deel van de) telecom-infrastructuur valt onder het toezicht van Agentschap Telecom is in overleg met de directeur-hoofdinspecteur van het agentschap besloten om het onderzoek gezamenlijk uit te voeren.

Het telecommunicatienetwerk van KPN

Het telecommunicatienetwerk waarin de storing plaatsvond betreft het landelijke SDH-netwerk van KPN. SDH staat voor *Synchronous Digital Hierarchy* en is een technologie die in de eerste helft van de jaren negentig is ontwikkeld. KPN zet het SDH-netwerk grotendeels in voor het transport van telefonie. Vaste telefonie is goed voor ongeveer tachtig procent van het verkeersvolume op het SDH-netwerk. Het overige verkeer komt enerzijds voor rekening van smalbanddiensten waaronder C2000, GSM en semafonie en anderzijds voor breedbanddiensten ten behoeve van corporate klanten als banken en overheid.

De storing trad op in een zogenaamde 'cross connect' (DXC). Een DXC is in het SDH-netwerk van KPN een knooppunt en opstappunt voor telecommunicatiediensten. Een belangrijke functie van een DXC is het routeren van verbindingen over het netwerk. Een DXC is in staat om verkeer over het netwerk te sturen, van de verzendende aansluiting naar de ontvangende aansluiting en terug.

Een DXC is dubbel uitgevoerd en bestaat uit twee identieke delen. Elk deel bevat een aantal componenten of kaarten. De voor dit incident meest relevante componenten zijn de matrix, klokkaart en voeding. Door hun dubbele uitvoering kan de functie van een actieve component op

[1] Aan deze 6200 transmissieverbindingen zijn ongeveer 200.000 klantaansluitingen verbonden.

ieder moment worden overgenomen door de passief meedraaiende component en terug. In geval van een storing of onderhoudswerkzaamheden kan geschakeld worden tussen de actieve en de passieve componenten. Hiermee wordt voorkomen dat er een onderbreking plaatsvindt in het telecommunicatieverkeer. Hoewel deze dubbele uitvoering zorgt voor grotere betrouwbaarheid, hebben diverse kaarten ook onderling afhankelijkheden.

Op een DXC kan een groot aantal verbindingen worden aangesloten. Het onderling koppelen van de verbindingen vindt plaats in een 'matrix', het verkeersplein van de DXC. Om het combineren van de verkeersstromen correct te laten plaatsvinden is synchronisatie tussen de verkeersstromen vereist. Om de verschillende verkeersstromen op elkaar te laten aansluiten is een klok nodig met een zeer stabiel signaal. Dit kloksignaal wordt opgewekt in een zogenaamde 'klokkaart'. Een DXC heeft elektriciteit (voeding) nodig om te kunnen functioneren. De voeding zorgt ervoor dat de binnenkomende spanning wordt teruggebracht naar een voor de componenten geschikte spanningswaarde.

Gezien de grote gevolgen die uitval heeft is de continuïteit van telecomdiensten van groot maatschappelijk belang. De samenleving mag daarom van KPN verwachten dat zij inspanningen verricht om uitval te voorkomen en bij incidenten effectief optreedt om uitval snel te verhelpen. Dit geldt voor de diensten van KPN in het algemeen, maar in het bijzonder voor het SDH-netwerk, waarvan veel vitale organisaties[2] en dienstverleners afhankelijk zijn. Van de afnemers van de diensten van KPN mag worden verwacht dat zij zich realiseren, dat (gedeeltelijke) uitval van systemen mogelijk is en dat zij zich hierop voorbereiden.

2 Het onderzoek

Het onderzoek moet antwoord geven op de vraag wat er precies is gebeurd rondom de uitval van de cross connect in de Waalhaven te Rotterdam in de nacht van 26 op 27 juli 2011 en wat de maatschappelijke gevolgen hiervan zijn geweest. Daarnaast moet het onderzoek uitwijzen in hoeverre KPN en vitale organisaties zijn voorbereid op een dergelijk incident.

Om het antwoord op deze vragen te kunnen geven zijn vier hoofdvragen geformuleerd.
1. Hoe is het risicomanagement bij KPN georganiseerd?
2. Welke reeks van gebeurtenissen heeft geleid tot de uitval van de 'cross connect' in de nacht van 26 op 27 juli 2011 in Rotterdam?
3. Wat waren de maatschappelijke effecten van de storing?
4. Hoe hebben de bij het incident betrokken vitale organisaties zich voorbereid op mogelijke uitval?

Bij dit onderzoek zijn twee toezichthouders betrokken: Agentschap Telecom en de Inspectie VenJ. Agentschap Telecom, onderdeel van het ministerie van Economische Zaken, Landbouw en Innovatie, heeft zich met name gericht op de aard, omvang en aanpak van de storing en op het risicomanagement van KPN. Bij dit onderzoek is gebruik gemaakt van de expertise van TNO. De Inspectie VenJ heeft onderzoek gedaan naar de maatschappelijke effecten van de storing in de

[2] Onder vitale organisaties worden in het kader van dit onderzoek verstaan: de betrokken veiligheidsregio's (Rotterdam-Rijnmond, Zuid-Holland Zuid, Hollands Midden en Zeeland), het Rotterdamse vervoersbedrijf RET, de Luchtverkeersleiding Nederland, de Luchthaven Rotterdam The Hague Airport en het Havenbedrijf Rotterdam, de waterleidingbedrijven Evides en Oasen, het Waterschap Hollandse Delta en het Hoogheemraadschap Schieland en Krimpenerwaard.

Waalhaven en zich hierbij gericht op de vier direct betrokken veiligheidsregio's en een aantal vitale organisaties.

Voor dit onderzoek zijn documenten bestudeerd en interviews gehouden met medewerkers van KPN en vertegenwoordigers van de betrokken veiligheidsregio's en een aantal vitale organisaties.

Het onderzoek heeft tot doel om inzicht te krijgen in het functioneren van de telecommunicatie-infrastructuur voor de vitale systemen van de Nederlandse samenleving en mogelijke knelpunten bloot te leggen. Het gaat hierbij vooral om de mate van kwetsbaarheid, maar minstens zo belangrijk is de vraag hoe herhaling kan worden voorkomen. Het onderzoek is bedoeld om lessen te trekken voor de toekomst.

3 Bevindingen

Op basis van het onderzoek komen Agentschap Telecom en de Inspectie VenJ tot de volgende bevindingen.

Risicobeheersing bij KPN

De activiteiten van KPN om telecommunicatienetwerken te beheersen zijn grotendeels beschreven in procedures en processen. KPN hanteert het begrip 'risico' als 'het effect van onzekerheid op het behalen van doelstellingen' en koppelt dit rechtstreeks aan het behalen van de Service Level Agreement (SLA) dat met de afnemer wordt afgesproken. Een SLA beschrijft onder andere welk beschikbaarheidsniveau KPN garandeert en wat de respons- en oplossingstijden zijn. De manier waarop KPN het beschikbaarheidsniveau berekent is voor de klant echter onduidelijk.

Om het beschikbaarheidsniveau van verbindingen te halen moet de continuïteit van het netwerk gewaarborgd blijven. Hiervoor hanteert KPN het proces Life Cycle Management (LCM). Dit proces omvat de gehele levenscyclus van een installatie, van aanschaf tot en met uitfasering en afvoer. De levenscyclus van het in dit onderzoek getroffen SDH-netwerk hangt grotendeels af van de beschikbaarheid van reserveonderdelen voor reparaties aan en vervanging van defect geraakte onderdelen. Het LCM is vooral afhankelijk van de waarborg dat de benodigde (hoeveelheid) reserveonderdelen beschikbaar zijn.

Afgezien van de beheersmaatregelen voor het LCM heeft KPN geen aanvullende risicobeheersmaatregelen getroffen. KPN heeft ook niet inzichtelijk gemaakt wat de gevolgen zijn van uitval van een DXC op de dienstverlening voor haar klanten of wat de maatschappelijke gevolgen zijn. Dit komt tot uiting in het feit dat het voor KPN pas dagen na het incident duidelijk is welke klanten in welke mate schade of hinder hebben ondervonden als gevolg van de storing. Als gevolg van het ontbreken van dit inzicht kan KPN niet duidelijk maken wat de totale impact is van het incident.

Oorzaak en aanpak van de storing

De storing in de cross connect in de Waalhaven te Rotterdam in de nacht van 26 op 27 juli 2011 is niet de eerste storing in dat knooppunt in die periode. Op 5 juni 2011 constateert KPN dat een onderdeel van dezelfde cross connect zich niet stabiel gedraagt. KPN besluit de volgende dag vervangingsonderhoud uit te voeren. Dit onderhoud slaagt maar gedeeltelijk en KPN acht verder onderhoud noodzakelijk om een aantal onderdelen te vervangen. Dit vindt plaats op 26 juli 2011. KPN leeft in de veronderstelling dat de dubbele uitvoering van onderdelen ervoor zorgt dat de cross connect zonder verstoring van de verbindingen blijft functioneren. Klanten worden daarom niet voor dit onderhoud gewaarschuwd. Dit blijkt een verkeerde inschatting te zijn.

Tijdens de werkzaamheden valt een groot aantal verbindingen uit, met aanzienlijke impact voor (vitale) klanten. Normaal gesproken zou de cross connect zichzelf moeten kunnen herstellen. Dit gebeurt echter niet. Een complete herstart is nodig om het systeem weer volledig operationeel te krijgen. Als gevolg van de herstart vallen voor de duur van de herstart (enkele uren) alle 6200 verbindingen van de cross connect uit. KPN heeft de betreffende klanten niet op de hoogte gesteld van de herstart.

Na het afronden van de herstart herstellen alle verbindingen zich weer. In de morgen van 27 juli 2011 lijkt de storing voorbij te zijn. Dezelfde avond echter ontstaat opnieuw een probleem, waardoor de dubbele redundantie niet meer functioneert. KPN besluit hierop om in een tweetal fasen zo snel mogelijk alle verbindingen van deze cross connect over te zetten naar een reserveapparaat van een nieuwer type. Op 22 augustus 2011 is de migratie volledig uitgevoerd, waarmee de dubbele uitvoering is hersteld.

Maatschappelijke effecten van de uitval

Het uitvallen van de verbindingen heeft een grote impact. In de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid, Hollands Midden en Zeeland vallen cruciale verbindingen uit. In drie veiligheidsregio's betreft dit de C2000-verbindingen[3] uit en in twee regio's[4] ook het alarmeringssysteem P2000. Ook functioneren een deel van het Nationaal Noodnet en verbindingen van het openbaar brandmeldsysteem niet meer.

De Veiligheidsregio's Rotterdam-Rijnmond en Zuid-Holland Zuid ondervinden de meeste last van de storing. Beide regio's schalen op naar GRIP 2 en de regio Rotterdam-Rijnmond op enig moment zelfs naar GRIP 4. Rotterdam-Rijnmond kiest hiervoor omdat – op het moment dat het maatschappelijk leven op gang komt – de storing nog niet is verholpen. De regio voorziet een aanzienlijke verkeerscongestie. Voor de veiligheidsregio's Hollands Midden en Zeeland is opschaling niet noodzakelijk. De veiligheidsregio's hebben bij hun activiteiten te maken met een gebrek aan informatie over het verloop van de storing. Het lukt KPN niet een indicatie te geven over de omvang en de duur van de uitval.

Uit het onderzoek komt naar voren dat de veiligheidsregio's adequaat reageerden op de storing en direct maatregelen troffen om de negatieve effecten van de storing, zowel op het functioneren van de eigen organisatie als het maatschappelijk leven, te minimaliseren. Doordat de uitval plaatsvond in de nachtelijke uren is deze aan velen onopgemerkt voorbij gegaan. Dit maakte dat de negatieve gevolgen beperkt waren. De veiligheidsregio's hebben van tevoren geen informatie ontvangen over de werkzaamheden. Ook communiceerde KPN niet over de 'koude herstart'. De veiligheidsregio's hadden dit wel van KPN verwacht om maatregelen te kunnen voorbereiden.

Van de andere vitale organisaties heeft de RET het meest direct te maken met de negatieve effecten van de uitval van de cross connect. Doordat de storing in de nachtelijke uren plaatsvindt blijft de overlast beperkt, maar dit wordt anders als de ochtendspits op gang komt en de storing nog niet is opgelost. De RET besluit om veiligheidsredenen het metroverkeer niet op te starten. De andere in het onderzoek betrokken vitale organisaties ondervinden beperkt of geen hinder en hoeven nauwelijks maatregelen te nemen. Zij treffen voorzorgsmaatregelen en volgen de ontwikkelingen nauwgezet om zo nodig in actie te ondernemen.

[3] Het betreft de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid en Hollands Midden.
[4] Het betreft de veiligheidsregio's Rotterdam-Rijnmond en Zuid-Holland Zuid.

Voorbereiding vitale organisaties op uitval

Uit het onderzoek blijkt dat de vier bij de storing betrokken veiligheidsregio's zich bewust zijn van het belang van continuïteitsmanagement voor de veiligheid in hun verzorgingsgebied. Drie van deze vier veiligheidsregio's[5] zijn ook daadwerkelijk bezig met het opstellen van een continuïteitsplan. Uit het onderzoek komt tevens naar voren dat de veiligheidsregio Zeeland ervoor kiest andere onderwerpen voorrang te geven en vooralsnog niet over te gaan tot het opstellen van een continuïteitsplan De inspecties vinden dit een opmerkelijke keuze. De continuïteit van de dienstverlening in relatie tot het niveau van veiligheid in het verzorgingsgebied maakt de noodzaak tot het hebben van een continuïteitsplan evident. De burger mag dit zonder meer van de overheid verwachten[6].

De vier betrokken veiligheidsregio's zijn tijdens de storing geconfronteerd met gedeeltelijke uitval van C2000. Dit communicatiesysteem voor de hulpdiensten is een landelijk systeem waarvan de veiligheidsregio's eindafnemers zijn. Veiligheidsregio's hebben slechts zeer beperkt invloed bij het optreden van storingen in het systeem en/of de afhandeling daarvan. Ook het monitoren van de storingen om, daarop anticiperend, maatregelen te kunnen treffen voor de operationele taakuitvoering, blijkt bijzonder lastig. Binnen de netwerkstructuur van C2000 heeft KPN vooral te maken met IVENT[7] en de vtsPN[8]. KPN beschouwt deze organisaties en niet de veiligheidsregio's, als directe klant. IVENT en de vtsPN ondervinden bij een storing echter niet de maatschappelijke druk van optredende problemen in de publieke veiligheid die veiligheidsregio's nadrukkelijk wel ervaren.

De andere vitale organisaties[9] kennen meer nog dan de veiligheidsregio's een hoge prioriteit toe aan continuïteitsmanagement. Naast bedrijfseconomische overwegingen speelt hierbij de maatschappelijke verantwoordelijkheid nadrukkelijk mee. Uit het onderzoek komt naar voren dat met name de vitale organisaties in de transportsector veiligheid hoog in het vaandel hebben. Continuïteit van de bedrijfsvoering is hieraan in principe ondergeschikt. De plannen voorzien er in dat - als de veiligheid niet kan worden gegarandeerd - het vlieg-, rail- en scheepvaartverkeer wordt stopgezet. Dit is ook tijdens de storing in de Waalhaven gebleken. De RET heeft het metroverkeer niet opgestart tot de storing was verholpen en het lossen van een vrachtschip, dat op het moment van de storing lag aangemeerd aan de LNG-terminal op de Maasvlakte, is uit voorzorg uitgesteld. De overige vitale organisaties hebben geen verdere actie hoeven te ondernemen, omdat de gevolgen van de storing voor hen beperkt waren.

Voor zover de vitale organisaties over een continuïteitsplan beschikken, houden zij hierin rekening met gedeeltelijke uitval van (telecom)voorzieningen. Totale uitval is in de meeste plannen niet opgenomen. Gelet op de ervaringen bij het incident in de Waalhaven zou verwacht mogen worden

---

[5] Het betreft de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid en Hollands Midden.

[6] In hoeverre de overige 21 veiligheidsregio's daadwerkelijk aan de slag zijn gegaan met continuïteitsmanagement is niet onderzocht. Of de situatie in de regio Zeeland wat dit onderwerp betreft uitzonderlijk is kan dan ook niet worden aangegeven. De inspecties kunnen alleen vaststellen dat de veiligheidsregio Zeeland afwijkt van de lijn die de andere drie betrokken veiligheidsregio's volgen.

[7] IVENT staat voor de bedrijfsgroep 'Informatievoorziening en –Technologie' van het ministerie van Defensie. IVENT levert de technische infrastructuur voor het systeem C2000.

[8] vtsPN staat voor 'voorziening tot samenwerking Politie Nederland'. De vtsPN is belast met het beheer en het onderhoud van C2000.

[9] Het betreft het Rotterdamse vervoersbedrijf RET, de Luchtverkeersleiding Nederland, de Luchthaven Rotterdam - The Hague Airport en het Havenbedrijf Rotterdam, de waterleidingbedrijven Evides en Oasen, het Waterschap Hollandse Delta en het Hoogheemraadschap Schieland en Krimpenerwaard.

dat de vitale organisaties de continuïteitsplannen op dit punt nog eens kritisch zouden bezien. Uit het onderzoek komt echter naar voren dat zij dit niet in de planning hebben opgenomen.

4 Conclusies

Op basis van het onderzoek komen Agentschap Telecom en de Inspectie VenJ tot de volgende conclusies.

Risicobeheersing bij KPN

- Er is sprake van onduidelijkheden rond Service Level Agreements. KPN baseert haar risicomanagement op het kunnen nakomen van de afspraken die in SLA's zijn vastgelegd. Het is echter voor de afnemers niet altijd duidelijk wat deze afspraken exact inhouden. Door deze onduidelijkheid kan bij klanten het idee leven dat zij een hoger serviceniveau krijgen dan dat zij daadwerkelijk met KPN hebben afgesproken. Dit kan ertoe leiden dat zij het risicomanagement baseren op verkeerde aannames en onbedoeld meer risico lopen.

- Het Life Cycle Management voor het SDH-netwerk voldoet aan de eisen die KPN daaraan zelf stelt. KPN wist echter al in 2002 dat de dubbele uitvoering van onderdelen niet in alle gevallen voldoet. Uit het onderzoek blijkt niet dat eerder voorgestelde verbetermaatregelen naar aanleiding van incidenten daadwerkelijk zijn uitgevoerd. Ook heeft KPN geen extra maatregelen getroffen om risico's op andere wijze af te dekken.

- KPN beschikt over bestanden waarin klantgegevens zijn opgeslagen. Er is echter geen systeem beschikbaar waarbij ingeval van een storing in het DXC-netwerk automatisch de van belang zijnde klantgegevens beschikbaar zijn. Hierdoor is KPN niet in staat gebleken bij deze storing de meest urgente verbindingen met voorrang te herstellen. Dit is nadelig voor het kunnen bepalen van de impact van het incident en het beperken van de gevolgen.

Oorzaak en aanpak van de storing

- KPN heeft het geplande onderhoud in de nacht van 26 op 27 juli 2011 voldoende voorbereid. Er is een draaiboek gebruikt en de daarin beschreven procedures zijn gevolgd. De onderhoudswerkzaamheden op zichzelf hebben geen onaanvaardbaar extra risico met zich meegebracht. Ook was de beschikbaarheid van reserve onderdelen toereikend.

- Nadat de verstoring was opgetreden heeft het escalatieproces van KPN (Be Alert) goed gefunctioneerd. Het incident is binnen een aanvaardbare tijd opgelost. De migratie van de verbindingen van de getroffen DXC naar een andere DXC is onder grote tijdsdruk uitgevoerd en goed verlopen. Het feit dat een vervangende DXC direct beschikbaar was heeft bijgedragen aan het verminderen van het potentiële risico op vervolguitval.

- Hoewel KPN een zogenaamd 'schoon werkproces' hanteert zijn in de DXC metaalresten aangetroffen. Hoewel niet mag worden geconcludeerd dat deze verontreiniging ten grondslag ligt aan de verstoring van de DXC, is hierdoor wel een onwenselijk risico ontstaan dat vermeden had kunnen worden.

- Door volledig te vertrouwen op de dubbele uitvoering van de apparatuur heeft KPN risico gelopen. KPN heeft bij het geplande onderhoud aan de DXC geen rekening gehouden met de mogelijkheid dat de DXC ook na de 'koude herstart' niet zou functioneren en dus volledig zou uitvallen. Een noodscenario ontbrak.

- Binnen Nederland zijn er nog 88 DXC's van hetzelfde type binnen de infrastructuur van KPN. Zonder tegenmaatregelen is er op deze locaties een vergelijkbare kans op storingen. De mogelijke impact hiervan is vooral in stedelijk gebied vergelijkbaar met de storing in de nacht van 26 op 27 juli 2011 in de Waalhaven te Rotterdam.

Maatschappelijke effecten van de uitval

- Vrijwel alle in het onderzoek betrokken vitale organisaties hebben in meerdere of mindere mate hinder of overlast ondervonden van de KPN-storing in de Waalhaven te Rotterdam. De primaire processen van de hulpverleningsdiensten en de overige onderzochte organisaties hebben niet te maken gehad met effecten die de gezondheid of veiligheid van personen direct aangetast hebben. Dat de maatschappelijke effecten van de storing gering waren was voor een belangrijk deel te danken aan het feit dat de storing in de nachtelijk uren plaatsvond. Uitval tijdens de dag- en avonduren had voor veel ernstiger hinder en overlast gezorgd.

- De storing trad op tijdens onderhoudswerkzaamheden en trof systemen die cruciaal zijn voor de hulpverleningsdiensten. In drie veiligheidsregio's viel het communicatiesysteem C2000 gedeeltelijk uit en in twee veiligheidsregio's voor een deel ook het alarmeringssysteem P2000. Ook delen van het Nationaal Noodnet en verbindingen van het openbaar brandmeldsysteem vielen uit.

- De veiligheidsregio's en de andere vitale organisaties hebben voortvarend gereageerd op de storing. In een aantal veiligheidsregio's is de crisisorganisatie gealarmeerd om adequaat te kunnen inspelen op de gevolgen van de uitval. De operationele hulpdiensten hebben maatregelen getroffen om bij incidenten de hulpverlening zo goed mogelijk doorgang te laten vinden.

- Binnen de onderzochte organisaties in de transportsector (de metro en het vlieg- en scheepvaartverkeer) worden geen concessies gedaan aan de veiligheid van het vervoer. Als de omstandigheden maken dat het transport niet veilig kan plaatsvinden, gebeurt dit niet of beperkt. Zo kan het metroverkeer worden stilgezet, het vliegverkeer worden afgebouwd of omgeleid en blijven schepen aan de kade of buitengaats. Op die manier is de veiligheid voor zowel passagiers als omgeving gewaarborgd. Hiermee geven de vitale organisaties op adequate wijze invulling aan hun maatschappelijke verantwoordelijkheid.

Voorbereiding vitale organisaties op uitval

- Alle onderzochte bedrijven en organisaties in de vitale sectoren beschikken over (delen van) een continuïteitsplan of een vergelijkbaar plan om de primaire 'vitale' processen zo ongestoord mogelijk doorgang te kunnen laten vinden. Bij de veiligheidsregio's zijn deze plannen nog volop in ontwikkeling. De andere vitale organisaties beschikken over meer uitgebreide continuïteitsplannen, die vooral zijn toegespitst op de primaire processen. Een aantal veiligheidsregio's beschikt wel over alternatieven, die in geval van uitval de communicatieverbindingen voor de operationele diensten beperkt kunnen overnemen.

- Veiligheidsregio's beseffen maar ten dele dat de uitval van communicatievoorzieningen zodanig grootschalig kan zijn, dat operationele hulpdiensten en andere vitale en/of maatschappelijke organisaties hun taken niet meer naar behoren kunnen uitvoeren. Organisaties als de RET, de Luchtverkeersleiding Nederland en het Havenbedrijf Rotterdam zijn zich hiervan meer bewust en hebben gedeeltelijke uitval ook in continuïteitsplannen opgenomen. Een continuïteitsplan dat rekening houdt met een totale uitval van communicatievoorzieningen is echter nergens aangetroffen.

5 Aanbevelingen

Op basis van het onderzoek doen Agentschap Telecom en de Inspectie VenJ de volgende aanbevelingen.

Aan KPN

- Leg de rekenmethoden achter de SLA-afspraken helder vast en deel deze met afnemers.
- Verkrijg inzicht in de toepassingen waarvoor klanten hun verbinding inzetten, zodat de prioriteiten van klanten beter inzichtelijk worden.
- Verbeter de koppeling tussen klantgegevens en verbindingsgegevens, zodat de impact van verstoringen sneller bepaald kan worden en bij het herstel rekening kan worden gehouden met de prioriteiten van klanten.
- Houd rekening met volledige en langdurige uitval van systemen en werk noodscenario's hiervoor uit.
- Neem alle passende, technische en organisatorische maatregelen om uitval in de andere 88 DXC's te voorkomen, waaronder - indien nodig - het preventief vervangen van (onderdelen van) klokkaarten.
- Informeer de veiligheidsregio's en andere vitale organisaties vooraf over onderhoudswerkzaamheden waarbij risico's bestaan voor het uitvallen van cruciale systemen.

Aan de besturen van de veiligheidsregio's en de andere vitale organisaties

- Wees u bewust van de kwetsbare positie van uw organisatie waar het gaat om de telecommunicatievoorzieningen. Ondanks een hoog SLA is (totale) uitval een reëel risico.
- Stel vast welke mate van uitval van het telecommunicatienetwerk acceptabel is, ervan uitgaande dat 100% zekerheid niet bestaat. Inventariseer welke alternatieve vormen van telecommunicatie geschikt zijn om bij (gedeeltelijke) uitval in de communicatiebehoefte te voorzien.
- Zorg voor een continuïteitsplan waarin, mede op basis van het risicoprofiel, aan de hand van crisisscenario's staat beschreven op welke manier cruciale processen doorgang kunnen vinden.
- Beoefen het scenario waarbij sprake is van (gedeeltelijke) uitval van communicatievoorzieningen
- Maak voor een optimale doorgang van de communicatie (ook tijdens crisisomstandigheden) afdoende afspraken met de aanbieders van telecommunicatievoorzieningen.
- Maak afspraken met KPN over het tevoren geïnformeerd worden over onderhoudswerkzaamheden, waarbij risico's bestaan voor het uitvallen van cruciale systemen.
- Verleen inzicht in de toepassingen waarvoor verbindingen worden ingezet, zodat gezamenlijk met KPN een rangorde van verbindingen bepaald kan worden.
- Stel u op de hoogte van de rekenmethoden van SLA-afspraken en kies voor cruciale verbindingen een SLA van voldoende hoog niveau.

Aan de minister van Defensie en de minister van Veiligheid en Justitie

- Draag er zorg voor dat IVENT en de vtsPN zich in geval van een storing nadrukkelijk als klant namens de veiligheidsregio's naar KPN toe manifesteren.

1 INLEIDING

1.1 Aanleiding

In de nacht van 26 op 27 juli 2011 pleegt KPN onderhoud aan het telecommunicatieknooppunt in de Waalhaven te Rotterdam. Tijdens dit onderhoud treedt een technische storing op in een zogenaamde 'cross connect'. Een cross connect is een belangrijk knooppunt in het netwerk van KPN. Het gevolg is dat 86 C2000-verbindingen en ongeveer 6200 andere transmissieverbindingen, vooral in gebruik voor telefonie en vaste dataverbindingen, gedurende bijna zeven uren worden verstoord.

Het uitvallen van de verbindingen heeft grote impact op de (vitale) infrastructuur binnen de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid, Hollands Midden en Zeeland. De storingen treffen onder meer verbindingen van en met banken, de verbinding tussen de meldkamer Zeeland en de ziekenhuizen, de luchtverkeersleiding van Rotterdam The Hague Airport, de metro in Rotterdam en de Rotterdamse haven. Ook automatische brandmelders en particuliere telefoonlijnen worden getroffen door uitval. De regio Zuid-Holland Zuid wordt geconfronteerd met storingen in de bereikbaarheid van het alarmnummer 112.

Nog diezelfde ochtend legt de Inspectie Veiligheid en Justitie (Inspectie VenJ) contact met de veiligheidsregio Rotterdam-Rijnmond en vraagt informatie op over de omvang en de impact van de storing. Uit de ter beschikking gestelde gegevens komt het beeld naar voren dat door de storing de veiligheid en de dienstverlening binnen de regio sterk negatief is beïnvloed. Het functioneren van onderdelen van de vitale infrastructuur is daarbij in het geding geweest. Het hoofd van de Inspectie VenJ besluit hierop een onderzoek in te stellen naar de uitval, de gevolgen en de risico's die dit heeft gehad voor het functioneren van de hulpdiensten en andere (publieke) diensten. Omdat het uitvallen van (een deel van de) telecom-infrastructuur valt onder het toezicht van Agentschap Telecom is in overleg met de directeur-hoofdinspecteur van het agentschap besloten om het onderzoek gezamenlijk uit te voeren.

Op 29 juli 2011 hebben de Kamerleden Van Raak (SP) en Kuiken / Van Dam (PvdA) vragen[10] gesteld aan de minister van Veiligheid en Justitie (VenJ). Bij zijn beantwoording geeft de minister aan dat hij de Inspectie VenJ heeft gevraagd onderzoek te doen naar het incident om zo inzicht te krijgen in het functioneren van de telecom-infrastructuur voor de vitale sectoren van onze samenleving.

1.2 Probleemanalyse

Het incident bij KPN tijdens onderhoudswerkzaamheden in de Waalhaven te Rotterdam in juli 2011 heeft een zodanige impact dat dit vragen oproept over de kwaliteit en de continuïteit van vitale systemen in de samenleving. Het onderzoek besteedt daarom aandacht aan de volgende thema's.

Het risicomanagement van KPN
KPN pleegt regelmatig onderhoud aan het netwerk. Het is de vraag in hoeverre KPN tevoren rekening houdt met mogelijke storingen en welke maatregelen zijn getroffen om uitval van het systeem te voorkomen. Het gaat hierbij om de betrouwbaarheid van de telecom-infrastructuur.

[10] Tweede Kamer der Staten-Generaal, kenmerk: 2011715828.

Daarnaast is de vraag aan de orde wat KPN doet om de klanten te informeren over de risico's en hen voor te bereiden op mogelijke uitval en welke maatregelen zijn genomen om herhaling te voorkomen.

Aard, omvang en aanpak van de storing
In het kader van dit thema is de belangrijkste vraag wat er in de zomer van 2011 precies is gebeurd. Hoe was het mogelijk dat tijdens reguliere onderhoudswerkzaamheden een cruciaal onderdeel van de telecom-infrastructuur van KPN uitviel? Het onderzoek moet antwoord geven op de vraag wat de aard en de oorzaak van de storing waren en hoe groot het gebied was dat te maken kreeg met de storing. Tevens is aan de orde welke maatregelen zijn genomen om de storing te verhelpen.

Maatschappelijke effecten van de storing
In de eerste plaats is het van belang vast te stellen welke impact de storing had op de vitale organisaties en diensten. Welke organisaties, diensten en infrastructuren zijn getroffen en waar in Nederland was het effect merkbaar? Het onderzoek moet informatie opleveren over welke vitale sectoren daadwerkelijk hinder of overlast hebben ondervonden en of sprake was van gevaar voor de (openbare) veiligheid.

Voorbereiding van de vitale sectoren op mogelijke uitval
Niet alleen van KPN maar ook de afnemers mag worden verwacht dat zij zich bewust zijn van wat hen kan overkomen. Daarom is het belangrijk vast te stellen of er tevoren een helder beeld is van wat er kan gebeuren en in hoeverre is men is voorbereid op mogelijke storingen. Beschikken de vitale organisaties over een risicoanalyse en een continuïteitsplan en welke maatregelen zijn genomen om herhaling te voorkomen?

1.3 Onderzoeksdoelstelling

Het onderzoek heeft tot doel om inzicht te krijgen in het functioneren van de telecommunicatie-infrastructuur voor de vitale systemen van de Nederlandse samenleving en mogelijke knelpunten bloot te leggen. Het gaat hierbij vooral om de mate van kwetsbaarheid, maar minstens zo belangrijk is de vraag hoe herhaling kan worden voorkomen.

Het onderzoek is bedoeld om lessen te trekken voor de toekomst. Het gaat niet om een onderzoek naar aansprakelijkheden. De analyse en conclusies zijn niet vervat in juridische termen en kunnen niet als zodanig worden beschouwd. Kwalificaties als 'onrechtmatig' komen in deze rapportage dan ook niet voor.

1.4 Onderzoeksvragen

Het onderzoek moet antwoord geven op de vraag wat er precies is gebeurd rondom de uitval van de cross connect in de Waalhaven te Rotterdam in de nacht van 26 op 27 juli 2011 en wat de maatschappelijke gevolgen hiervan zijn geweest. Daarnaast moet het onderzoek uitwijzen in hoeverre KPN en vitale organisaties zijn voorbereid op een dergelijk incident.

Om het antwoord hierop te kunnen geven zijn voor het onderzoek **vier hoofdvragen** geformuleerd.

1. *Hoe is het risicomanagement bij KPN georganiseerd?*
   Hierbij komt de vraag aan de orde op welke manier KPN is voorbereid op uitval. Wat is de mate van redundantie en welke procedures en processen zijn van toepassing bij de uitvoering van

reparatiewerkzaamheden. Zijn de afnemers op de hoogte van de storingsgevoeligheid van de apparatuur en wat heeft KPN hierover gecommuniceerd? Ook wordt hierbij betrokken welke maatregelen zijn of worden genomen om herhaling te voorkomen.

2. *Wat was de oorzaak van de uitval van de 'cross connect' in de nacht van 26 op 27 juli 2011 in Rotterdam en hoe is de storing aangepakt?*
   Hierbij wordt beschreven wat er precies is gebeurd rondom de uitval van de cross connect in de Waalhaven te Rotterdam. Naast de oorzaken van de uitval gaat het bij deze tweede hoofdvraag om de aard en de omvang van het incident. Tevens wordt bezien op welke manier KPN het incident heeft aangepakt, welke maatregelen zijn genomen om de storing ongedaan te maken.

3. *Wat waren de maatschappelijke effecten van de storing?*
   Hierbij gaat het om de vraag welke organisaties, diensten en infrastructuren in welke delen van Nederland zijn getroffen door de storing. Was er sprake van gevaar voor de openbare veiligheid? Bij dit thema wordt in het bijzonder aandacht besteed aan de betrokken vitale organisaties.

4. *Hoe hebben de bij het incident betrokken vitale organisaties zich voorbereid op mogelijke uitval?*
   Voor de continuïteit van vitale organisaties is het van belang dat zij zijn voorbereid op mogelijke uitval. Wat is er specifiek geregeld in verband met mogelijk uitval van telecom-voorzieningen en zijn hierover afspraken gemaakt met KPN? Ook komt aan de orde welke maatregelen zijn of worden genomen om herhaling in de toekomst te voorkomen.

1.5 Afbakening en afstemming

Dit onderzoek is uitgevoerd door twee toezichthouders: Agentschap Telecom en de Inspectie Veiligheid en Justitie (Inspectie VenJ). Vanaf het begin hebben beide toezichthouders intensief samengewerkt.

Focus Agentschap Telecom

Agentschap Telecom, onderdeel van het ministerie van Economische Zaken, Landbouw en Innovatie, richt zich specifiek op de onderzoekdelen die te maken hebben met de continuïteit van het telecommunicatienetwerk. Het gaat daarbij vooral op het beantwoorden van de vraag naar de oorzaak en omvang van de storing en de technische kans op een herhaling. Bij dit laatste aspect legt het agentschap de nadruk op het bepalen van de mate van redundantie, een factor die de kans op herhaling kan verkleinen.

Voor dit onderzoekdeel heeft Agentschap Telecom de werking van de technische installaties onderzocht en interviews gehouden met medewerkers van KPN die vanuit verschillende competenties betrokken zijn bij het getroffen netwerk. Hierbij heeft het agentschap gebruik gemaakt van de expertise van TNO.

Focus Inspectie Veiligheid en Justitie

De storing in de Waalhaven heeft ook effect gehad op het maatschappelijk leven en de openbare veiligheid. Cruciale verbindingen van de hulpverleningsdiensten vielen uit en ook andere vitale organisaties hadden in meer of mindere mate te maken met uitval. De Inspectie VenJ richt zich in dit onderzoek specifiek op deze aspecten. Hiervoor zijn de meest betrokken veiligheidsregio's en een aantal vitale organisaties bezocht en is gekeken hoe deze organisaties met de storing zijn

omgegaan en op welke manier zij waren voorbereid op een dergelijk incident. In dit verband is ook bezien of de vitale organisaties over een continuïteitsplan beschikken.

Het onderzoek richt zich op de gevolgen voor het publieke deel van de getroffen verbindingen en gaat daarbij uit van een driedeling. In de eerste plaats gaat het om verbindingen die aantoonbaar onderdeel uitmaken van de vitale infrastructuur en die met name zijn genoemd in de *'(2e) inhoudelijke analyse bescherming vitale infrastructuur'* [11]. Een voorbeeld hiervan is de sector transport binnen de Mainport Rotterdam. In de tweede plaats richt het onderzoek zich op C2000 en P2000 als cruciale verbindingen voor de openbare veiligheid. Ten slotte worden onderdelen betrokken die hier geen direct verband hebben met openbare veiligheid, maar wel (andere) aanzienlijke belangen vertegenwoordigen. Het gaat bijvoorbeeld om het openbaar (brand)meldsysteem (OMS).

1.6 Methode van onderzoek

Agentschap Telecom en de Inspectie VenJ hebben het onderzoek uitgevoerd in de periode augustus 2011 – februari 2012. Agentschap Telecom heeft zich gericht op de activiteiten van KPN, de Inspectie VenJ heeft de betrokkenheid van de desbetreffende veiligheidsregio's en andere vitale organisaties onderzocht. Agentschap Telecom heeft zich bij haar onderzoek laten ondersteunen door TNO.

Onderzoek KPN

Agentschap Telecom heeft bij KPN relevante documenten opgevraagd. In totaal heeft KPN 183 documenten aangeleverd. Daarnaast zijn interviews gehouden met functionarissen van KPN. Voor de interviews is een interviewprotocol opgesteld. De verslagen van de interviews zijn voor akkoord voorgelegd aan de geïnterviewden.

In eerste aanleg is gesproken met technische medewerkers die direct bij het incident betrokken waren, om informatie te verkrijgen over het feitelijke verloop van het incident. Vervolgens is gesproken met de verantwoordelijke managers, om ook inzicht te krijgen in de achterliggende beheersprocessen.

De vragenlijst is vooraf aan de deelnemers toegezonden. Voor alle genoemde feiten is schriftelijk bronmateriaal gevraagd. Voor elke gedane bewering is bevestiging gevraagd van minstens een andere geïnterviewde. Aan elk interviewverslag is een actiepuntenlijst toegevoegd, waarop staat vermeld welke acties nog moeten worden ondernomen in het kader van het onderzoek. Dit kan zijn het nazoeken van bepaalde feiten of het toesturen van bronmateriaal. In totaal zijn tien interviews gehouden. Alle interviewverslagen zijn door KPN goedgekeurd.

De bevindingen over KPN, zoals opgenomen in de paragrafen 3.1. en 3.2 zijn ter controle op feitelijke onjuistheden toegezonden aan KPN. Ook is KPN in de gelegenheid gesteld een mondelinge toelichting te geven op de reactie op de concept-bevindingen. Naar aanleiding van de opmerkingen van KPN is de tekst op onderdelen aangepast.

---

[11] In 2005 is voor het eerst een inhoudelijke analyse over de bescherming van de vitale infrastructuur in Nederland aan de Tweede Kamer aangeboden. Er is toen toegezegd om dit in 2009 te herhalen. Deze rapportage beschrijft een inhoudelijke analyse van de stand van zaken eind 2009.

Onderzoek vitale sectoren

Voor het onderzoek bij de vitale sectoren die te maken hebben gehad met de KPN-storing heeft de Inspectie VenJ interviews gehouden met vertegenwoordigers van de betrokken organisaties die inhoudelijke kennis van de uitval hadden en/of operationeel verantwoordelijk waren voor de aanpak van het incident. De betrokken organisaties hebben tevens studierapporten en andere operationele documenten ter beschikking gesteld aan de Inspectie VenJ.

Ook zijn personen geïnterviewd die verantwoordelijk zijn voor of betrokken zijn bij het continuïteitsmanagement van de betreffende organisaties. Aan hen is verzocht om bij de interviews de continuïteitsplannen (voor zover aanwezig) ter inzage voorhanden te hebben. De gespreksverslagen zijn ter verificatie toegezonden aan de geïnterviewden. De opmerkingen zijn verwerkt in de definitieve tekst van het rapport.

1.7 Leeswijzer

Dit rapport bestaat uit vijf hoofdstukken, voorafgegaan door een managementsamenvatting. Het eerste hoofdstuk bevat de inleiding, waarna in hoofdstuk 2 het onderzoekskader en enkele technische begrippen worden beschreven. Het derde hoofdstuk bevat de bevindingen en de analyse van Agentschap Telecom en de Inspectie VenJ. In de eerste twee paragrafen komen de risicobeheersing van KPN en de aanpak van het incident op 27 juli 2011 aan de orde. De derde en vierde paragraaf van het derde hoofdstuk zijn gewijd aan de maatschappelijke effecten en de voorbereiding van de vitale sectoren. Hoofdstuk 4 bevat de conclusies en in het vijfde hoofdstuk zijn de aanbevelingen opgenomen.

2 ONDERZOEKSKADER

In dit hoofdstuk wordt beschreven welk onderzoekskader Agentschap Telecom en de Inspectie VenJ hanteren bij dit onderzoek. Voor een goed begrip van de inhoud van dit rapport wordt in paragraaf 2.1 eerst enige technische achtergrondinformatie verstrekt over het telecommunicatienetwerk. In paragraaf 2.2 wordt het onderzoekskader nader beschreven.

2.1 Begrippen telecommunicatie

Het SDH-netwerk van KPN

Het telecommunicatienetwerk waarin de storing plaats vindt is het landelijke SDH-netwerk van KPN. SDH staat voor Synchronous Digital Hierarchy en is een technologie die in de eerste helft van de jaren negentig ontwikkeld is.
KPN zet het SDH-netwerk grotendeels in voor het transport van telefonie. Vaste telefonie is goed voor ongeveer tachtig procent van het verkeersvolume op het SDH-netwerk. Het overige verkeer komt enerzijds voor rekening van smalbanddiensten waaronder C2000, GSM en semafonie; en anderzijds voor breedbanddiensten ten behoeve van corporate klanten als banken en overheid.

DXC: de cross connect

Een digital cross connect (DXC) is in het SDH-netwerk een knooppunt en opstappunt voor telecommunicatiediensten. Een belangrijke functie van een DXC is het routeren van verbindingen over het SDH-netwerk van KPN. Een DXC is in staat om verkeer over het SDH-netwerk te sturen, van de verzendende aansluiting naar de ontvangende aansluiting en terug.
Een DXC is dubbel uitgevoerd en bestaat uit twee identieke delen. Elk deel bevat een aantal componenten of kaarten. De voor dit incident meest relevante componenten zijn de matrix, klokkaart en voeding. Door hun dubbele uitvoering kan de functie van een actieve component op ieder moment worden overgenomen door de passief meedraaiende component en terug. In geval van een storing of onderhoudswerkzaamheden kan geschakeld worden tussen de actieve en de passieve componenten. Hiermee wordt voorkomen dat er een onderbreking plaatsvindt in het telecommunicatieverkeer. Hoewel deze dubbele uitvoering zorgt voor hogere betrouwbaarheid, hebben diverse kaarten ook onderling afhankelijkheden.

Matrix

Op een DXC kan een groot aantal verbindingen worden aangesloten. Het onderling koppelen van verbindingen vindt plaats in de matrix, het verkeersplein van de DXC. Met name de klokfunctie is van belang om het verkeer ongestoord te kunnen routeren over het verkeersplein.

Klokkaart

Om het combineren van de verkeersstromen correct te laten plaatsvinden is synchronisatie tussen de verkeersstromen vereist. Als de verschillende verkeersstromen van verschillende klokken gebruik zouden maken dan sluit het niet op elkaar aan en stokt het verkeer. Hiertoe is een klok nodig met een zeer stabiel kloksignaal. Dit kloksignaal wordt opgewekt in een klokkaart. Binnen een klokkaart is de oscillator een cruciaal onderdeel om een stabiel kloksignaal te genereren.

Voeding

Een DXC heeft elektriciteit nodig om te kunnen functioneren. De functie van een voeding is om de binnenkomende hogere spanning terug te brengen naar de voor de componenten geschikte lagere spanningswaarde.

2.2 Het onderzoekskader

Agentschap Telecom en de Inspectie VenJ hebben bij het uitvoeren van het onderzoek vanuit twee invalshoeken gekeken naar het incident in de Waalhaven te Rotterdam.

De eerste invalshoek betreft de continuïteit van de telecommunicatie. Aanbieders van telecommunicatiediensten moeten de continuïteit van de dienstverlening zo goed mogelijk kunnen waarborgen naar de afnemers toe. Het optreden van KPN is vooral vanuit deze invalshoek bezien.

De tweede invalshoek heeft betrekking op de afnemers van telecommunicatiediensten: burgers, vitale organisaties en overheidsinstanties. Zij zijn zich veelal niet bewust van de toenemende afhankelijkheid van telecommunicatie. Deze 'telekwetsbaarheid' komt met name bij het onderzoek naar de vitale organisaties aan de orde.

Onderzoek KPN

De Nederlandse wetgeving bevat op dit moment geen bepalingen die rechtstreeks van toepassing zijn op het Waalhaven-incident. Om de continuïteit te waarborgen of waar nodig te verhogen treedt medio 2012 nieuwe wetgeving in werking voor de gehele telecommunicatiesector. Sinds 2010 bestaat er een (gewijzigd) Europees Regelgevend Kader voor Elektronische Communicatie, the New Regulatory Framework. In dit nieuw regelgevend kader (NRK, of NRF in het Engels) zijn voor aanbieders twee verplichtingen opgenomen die beide tot doel hebben de veiligheid en integriteit van de eigen netwerken of diensten te borgen. Het gaat hierbij om een *zorgplicht* continuïteit en een *meldplicht* continuïteit (zie kader).

Zorgplicht continuïteit	**Meldplicht continuïteit**
Aanbieders van openbare elektronische communicatienetwerken en -diensten zijn verplicht *passende* technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en integriteit van netwerken en diensten te beheersen. Voor aanbieders van openbare telefoniediensten geldt zelfs de verplichting om in het geval van een technische storing of uitval van het elektriciteitsnetwerk alle noodzakelijke maatregelen te treffen, ongeacht de kosten. Het doel hierbij is om de continuïteit en beschikbaarheid van netwerken en diensten zoveel als mogelijk te waarborgen. Het gaat hierbij om inbreuken op de veiligheid en een verlies aan integriteit van het netwerk en/of de dienst.	Aanbieders van openbare elektronische communicatienetwerken en -diensten zijn verplicht om bij inbreuken op de veiligheid en/of een (gedeeltelijk) verlies aan integriteit melding te maken van dit incident bij Agentschap Telecom.

Met de implementatie van deze Europese regelgeving in de Telecommunicatiewet in de zomer van 2012 wordt wetgeving van kracht die nadere regels stelt aan telecomaanbieders over de continuïteit van hun diensten. Deze wetgeving was op het moment van het incident in de Waalhaven nog niet van kracht en is daarom voor dit onderzoek buiten beschouwing gelaten. Het onderzoek richt zich dan ook niet op de vraag of wet- of regelgeving is overtreden.

Telecomdiensten spelen een belangrijke rol in het maatschappelijk verkeer. De samenleving mag daarom van elke grote telecomaanbieder verwachten dat deze zich als een goed 'huisvader' gedraagt en de nodige inspanningen verricht om uitval te voorkomen en bij incidenten effectief optreedt om uitval snel te verhelpen.
KPN onderschrijft deze opvatting en refereert hier ook aan in haar missie[12]: *'Onze klanten vertrouwen erop dat wij dit doen met de kwaliteit en betrouwbaarheid die zij inmiddels van ons gewend zijn'*. En ook: *'We zijn ons bewust van onze verantwoordelijkheid jegens de maatschappij: wij gebruiken onze kennis en technologie om bij te dragen aan het welzijn van al onze belanghebbenden'*.

In het Maatschappelijk verslag 2011 (blz. 19) geeft KPN aan dat de kern van de strategie is 'de ambitie om de beste dienstverlener te worden: door het beste netwerk en de beste service'. Zo wil KPN in de samenleving staan als een transparante en betrouwbare dienstverlener die nauw verbonden is met de samenleving en zijn klantbeloftes waarmaakt.

KPN mag er dus aan worden gehouden dat zij rekening houdt met maatschappelijke belangen en met belangen van haar klanten. Ingeval KPN deze belangen niet kent mag worden verwacht dat zij zich enige moeite getroost om die belangen te leren kennen.

Onderzoek vitale organisaties

De samenleving is steeds meer afhankelijk van elektriciteit, ICT en telecommunicatievoorzieningen. Deze toenemende afhankelijkheid maakt de samenleving in toenemende mate kwetsbaar. Een uitval of verstoring heeft grote gevolgen voor het dagelijks leven. Om maatschappelijke ontwrichting te voorkomen is daarom het belangrijk dat de overheid en bedrijven vitale producten en diensten kunnen leveren, ook tijdens een incident, ramp of crisis. Met behulp van continuïteitsplannen kunnen bedrijven en overheidsinstanties er voor zorgen dat zij blijven functioneren.

Onder verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties is in 2007 onderzoek verricht naar risico's voor de nationale veiligheid. In vervolg hierop heeft de overheid bijvoorbeeld gewerkt aan de voorbereiding van vitale sectoren op een mogelijke grieppandemie. Sinds eind 2009 hebben bijna alle relevante organisaties, zoals ziekenhuizen, energiebedrijven en overheidsinstanties een continuïteitsplan dat rekening houdt met een grieppandemie. Uit onderzoek in 2008 blijkt dat vitale sectoren beter beschermd moeten worden tegen uitval van communicatie (ICT) en elektriciteit.
De minister gaf aan dat in 2011 ook deze onderwerpen moeten worden meegenomen in de continuïteitsplannen van organisaties die in hoge mate afhankelijk zijn van ICT en elektriciteit[13].

---

[12] Zie de website van KPN www.kpn.com/corporate.
[13] Zie ook de tweede voortgangsbrief Nationale Veiligheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer d.d. 5 juni 2009.

Het ministerie van Veiligheid en Justitie stimuleert organisaties met een vitale functie en biedt hen een pakket aan om continuïteitsmanagement te bevorderen. In december 2010 verscheen de handleiding 'Continuïteitsmanagement voor organisaties met een vitale functie'. Deze handleiding beoogt organisaties bewust maken van de risico's, het belang van continuïteitsmanagement te onderbouwen en organisaties te ondersteunen bij het invullen en inbedden van continuïteitsmanagement en daarmee het reduceren van de risico's. De handleiding richt zich met name op uitval van ICT en elektriciteit, maar wijst er tevens op gewezen dat er ook andere continuïteitsrisico's zijn en dat de handleiding handvatten biedt om de organisatie te wapenen tegen allerlei bedreigingen.

Daarnaast hebben organisaties ook een eigenstandige verantwoordelijkheid als het gaat om de continuïteit van hulp- en dienstverlening en dienen zij aandacht te hebben voor het continuïteitsmanagement van de organisatie.

3 BEVINDINGEN EN ANALYSE

Het derde hoofdstuk is onderverdeeld in vier paragrafen. In de eerste paragraaf wordt nader ingegaan op het risicomanagement van KPN, waarbij met name aandacht wordt besteed aan Life Cycle Management en de Service Level Agreements. In paragraaf 3.2 worden de gebeurtenissen rond het incident op hoofdlijnen beschreven. In deze paragraaf wordt ook de oorzaak van de uitval beschreven, alsmede de aanpak van het incident door KPN. In de derde paragraaf van dit hoofdstuk wordt aandacht besteed aan de maatschappelijke effecten, waarbij de inspecties zich met name richten op een aantal vitale sectoren. In paragraaf 3.4 komt de voorbereiding van deze vitale sectoren aan de orde.

3.1 Risicobeheersing bij KPN

De samenleving verwacht van KPN goed huisvaderschap. In het bijzonder zal KPN inspanningen moeten verrichten om uitval van telecomdiensten te voorkomen en bij incidenten snel en effectief de dienstverlening te herstellen. Hierbij dient zij rekening te houden met de belangen van klanten en van de maatschappij. Dat vraagt om zorgvuldige risicobeheersing. In deze paragraaf wordt toegelicht hoe KPN hiermee omgaat.

De literatuur[14] beschrijft risicobeheersing als een cyclus. Eerst worden risico's beoordeeld, dan worden beheersmaatregelen gekozen en uitgevoerd en vervolgens wordt het effect beoordeeld. Dan vervolgt de cyclus met het opnieuw beoordelen van risico's, rekening houdend met de ervaringen van de eerste ronde van de cyclus.

Een risicobeoordeling begint met het inventariseren van te beschermen belangen. Zodra deze belangen zijn bepaald kan een omgevingsschets worden gemaakt, gevolgd door identificatie van risico's, een analyse daarvan (wat zijn de eigenschappen van ieder risico) en tenslotte een risico-evaluatie, waarin elk risico een waarde krijgt toegekend.

Zijn zowel de waarschijnlijkheden als de gevolgen van risico's goed numeriek in te schatten, dan wordt vaak de statistische verwachting (kans x effect) van het risico als maatstaf gehanteerd. Tegenwoordig is echter ook een bredere definitie van risico gangbaar: het effect van onzekerheid op het behalen van doelstellingen. Hoewel in het onderzoek geen eenduidige definitie is aangetroffen van wat KPN bedoelt met 'risico', lijkt zij de moderne definitie te hanteren. Deze omschrijving wordt ook in het publieke jaarverslag 2011 genoemd. De doelstelling is om te voldoen aan de afspraken die met klanten zijn gemaakt.

Het risicomanagement binnen KPN is ingericht rondom twee centrale zaken: Life Cycle Management en Service Level Agreements. Het Life Cycle Management zorgt ervoor dat afgesproken niveaus van dienstverlening gehaald kunnen worden; Service Level Agreements bepalen wat het gewenste niveau van dienstverlening moet zijn. Deze onderwerpen komen hierna aan de orde.

[14] Zie bijvoorbeeld de internationale ISO 31.000 norm.

3.1.1 Life Cycle Management

Inleiding

Life Cycle Management (LCM) beheert de hele levenscyclus van een installatie, van het besluit tot aanschaf tot en met uitfasering en de definitieve afvoer van de installatie. Het doel van Life Cycle Management is om bewuste keuzes te maken over de operationele inzet van installaties, om zo de financiële en technische risico's beheersbaar te houden. Specifieke vragen die tijdens Life Cycle Management aan de orde komen zijn: 'Wanneer moet tot vervanging van een installatie worden besloten?' en 'Welk onderhoudsniveau is op dit moment gewenst?'.

Werkwijze KPN

KPN hanteert een beperktere definitie van Life Cycle Management dan in de literatuur gebruikelijk is, namelijk het waarborgen van de continuïteit van een platform (in dit geval het SDH-netwerk).

De regie over Life Cycle Management wordt gevoerd door een LCM Advisory Board, waarin vertegenwoordigers van zowel technische als commerciële afdelingen zitten. De LCM Advisory Board hanteert als uitgangspunt dat apparatuur-storingen opgelost worden door reparaties en dat de beschikbaarheid van reserveonderdelen gegarandeerd moet zijn. De LCM Advisory Board stelt dat een kans van 1 procent dat een benodigd onderdeel niet op voorraad is nog acceptabel is. In de rekenmodellen houdt KPN rekening met het aantal installaties in het veld, eigen ervaringscijfers over uitval van onderdelen en verhoogde uitvalskansen door veroudering. De LCM Advisory Board gaat er van uit dat de huidige SDH-installaties tot 2015 operationeel moeten kunnen blijven.

Bevindingen en analyse

Life Cycle Management is een relatief nieuw proces binnen KPN. Het is in 2009 opgezet, vooral om de continuïteit van het SDH-netwerk te borgen. Het LCM-proces maakt gebruik van overzichten en hulpmiddelen die ook vóór 2009 al in gebruik waren.

KPN is van mening dat met de beschikbaarheid van reserveonderdelen de risicobeheersing voldoende is geborgd. Uitval van één onderdeel heeft in de meeste gevallen geen invloed op de dienstverlening, doordat de meeste DXC-functies dubbel zijn uitgevoerd, aldus KPN. Uitval kan hooguit een beperkt aantal klanten raken. Sturen op alleen de beschikbaarheid van reserveonderdelen is onder deze aanname volgens KPN dan ook voldoende.

In 2002 is er echter een aantal incidenten geweest waarin toch een complete DXC uitviel. KPN heeft naar aanleiding daarvan een aantal verbetervoorstellen besproken. Deze voorstellen zouden gezorgd hebben voor aanscherping van de werkprocedures, het doen van preventief onderhoud, verbetering van de bewaking van de apparatuur en van het opleidingsniveau van personeel. Uit het onderzoek is niet gebleken welke van deze verbetervoorstellen daadwerkelijk zijn uitgevoerd.

Het LCM-proces heeft de beschikbaarheid van alle reserveonderdelen ten tijde van het incident afdoende geborgd. Hoewel ten tijde van het eerste onderhoud in de nacht van 5 op 6 juni geen benodigde correct functionerende kabel ter plaatse aanwezig was, waren alle vitaal geachte reserve onderdelen in voldoende mate beschikbaar voor KPN.
Ook tot aan 2015 is de beschikbaarheid van reserveonderdelen voor DXC's zodanig dat de grens van hooguit 1 procent kans dat een onderdeel niet beschikbaar is, wordt gehaald. KPN kan dit doel bereiken doordat het gebruik van het SDH-netwerk afneemt. Door overblijvende verbindingen te concentreren, kunnen DXC's geheel vrijgemaakt worden. De onderdelen daarvan komen dan beschikbaar als reserveonderdelen voor die DXC's die nog wel actief blijven.

Na 2015 zullen sommige onderdelen echter niet meer op voorraad zijn. Tegelijkertijd is KPN zich ervan bewust dat het SDH-netwerk tot 2020 operationeel moet blijven ten behoeve van vaste telefonie. De LCM Advisory Board heeft in februari 2011 plannen besproken om alle dan nog in gebruik zijnde DXC's te vervangen door nieuwere types. Daarmee zal dan ook tussen 2015 en 2020 de continuïteit gewaarborgd zijn.

3.1.2 Service Level Agreements

Een Service Level Agreement (SLA) is een afspraak tussen KPN en een klant of leverancier, maar kan ook bestaan tussen twee bedrijfsonderdelen binnen KPN. Een SLA beschrijft onder andere welk beschikbaarheidsniveau KPN garandeert en wat de responstijden en oplossingstijden zijn. Een SLA bevat ook leveringstermijnen en opzegtermijnen. Deze termijnen zijn voor dit onderzoek niet relevant. Een SLA kan ook een boeteclausule bevatten. KPN betaalt dan een voorgeschreven geldbedrag terug aan de betrokken afnemer als de afspraken in de SLA niet gehaald worden. De hoogte van zulke boetes is afhankelijk van de ernst van de overschrijding en is aan een maximum gebonden.

KPN legt met klanten soms aanvullende of striktere afspraken vast. Dit is eerder uitzondering dan regel; voor de meeste klanten is het standaard SLA voldoende.

De afspraken die KPN hanteert, vallen uiteen in drie domeinen:
1. Toezeggingen die de *klant* ontvangt van de commerciële afdeling Zakelijke Markt.
2. Toezeggingen die de *afdeling Zakelijke Markt* ontvangt van de afdelingen Technisch Productmanagement en Netwerk, IP & Access, die de technische realisatie voor hun rekening nemen.
3. Toezeggingen die *afdeling Netwerk, IP & Access* ontvangt van leveranciers voor onderhoud.

Deze domeinen zijn hierna verder uitgewerkt.

3.1.2.1 De klant

Zakelijke klanten sluiten een contract en bijbehorend Service Level Agreement af met de afdeling Zakelijke Markt van KPN.

Werkwijze KPN

De toezeggingen die de afdeling Zakelijke Markt doet aan de klanten zijn vastgelegd in vaste Service Level Agreements. De klant heeft enige invloed op de inhoud van een SLA. Voor de beschikbaarheid van aansluitingen op het SDH-netwerk biedt KPN twee standaardpakketten:

Type	Beschikbaarheid	Storingshersteltijden
Premium A	99,90%	90% ≤ 4 uur, 100% ≤ 8 uur
Premium B	99,98%	100% ≤ 2 uur

Het is aan de klant om te kiezen welke variant hij afneemt, maar de beschikbaarheidswaarden en storingshersteltijden zelf zijn niet vrij te kiezen. Als een klant een dienstenniveau wenst dat daarvan afwijkt, dan kan KPN specifiek daarvoor afwijkende procedures inrichten.

Over het voorafgaand informeren van klanten over gepland onderhoud door KPN is met klanten meestal geen afspraak gemaakt. Wel heeft KPN met IVENT, de bedrijfsgroep Informatievoorziening en –Technologie van het ministerie van Defensie, aanvullende afspraken gemaakt[15].

KPN rekent voor de storingshersteltijd de periode tussen het moment dat de klant de storing meldt en het moment dat KPN de klant bericht dat de storing is verholpen. Dit betekent dat als de klant de storing niet meldt, KPN er ook niet van uit gaat dat er sprake is van een storing die invloed heeft op de SLA.
Het is in het onderzoek niet duidelijk geworden hoe KPN de beschikbaarheid berekent. Agentschap Telecom gaat er in dit rapport van uit dat niet-beschikbaarheid op dezelfde wijze wordt gedefinieerd als een storing, namelijk van moment van melden door de klant tot aan het moment van afmelden door KPN.

Bevindingen en analyse

Een klant die een SDH-dienst afneemt kan kiezen uit twee varianten: Premium A met een beschikbaarheid van minstens 99,90% en Premium B met een beschikbaarheid van minstens 99,98%. Een beschikbaarheid van 99,90% betekent dat aan de SLA wordt voldaan als op maandbasis de dienst hooguit drie kwartier niet beschikbaar is. Er zijn echter vier factoren die, voor de klant, tot onverwachte interpretatieverschillen kunnen leiden.

1. KPN rekent met een gemiddelde beschikbaarheid van alle verbindingen onder een contract, niet met de beschikbaarheid per verbinding. Als een klant tien verbindingen afneemt, kan de uitval op één verbinding dus vertienvoudigen terwijl KPN binnen de SLA afspraken blijft, mits alle andere verbindingen volledig beschikbaar blijven.
2. In het onderzoek heeft het agentschap niet met zekerheid kunnen achterhalen of gepland onderhoud buiten de beschikbaarheid valt. Indicaties uit diverse documenten zijn dat (gepland en ongepland) uitval tijdens de standaard onderhoudsperiodes (05:00 – 07:00 uur) niet meetelt. Zeker is dat het aantal keren dat gebruik gemaakt wordt van de onderhoudsperiodes niet gelimiteerd is. Als gepland onderhoud buiten de berekeningen wordt gehouden, kan de niet-beschikbare tijd nog hoger zijn voordat de limieten in de SLA worden overschreden.
3. Ook is niet uit te sluiten dat uitval die door de klant niet wordt gemeld buiten de statistieken wordt gehouden. Het Service Level Agreement bevat een restitutieclausule; de bewijslast ligt hierbij bij de klant. Met andere woorden; een incident lijkt voor KPN alleen een incident te zijn als de klant het incident bij KPN meldt.
4. KPN sluit in haar SLA bovendien een aantal omstandigheden uit. Omstandigheden waarin het juist voor klanten die een vitale maatschappelijke rol vervullen essentieel kan zijn om over communicatieverbindingen te beschikken:
   […] *calamiteiten (w.o. brand, neerstortend vliegtuig, schadelijke stoffen, explosiegevaar), files die redelijkerwijs niet te ontwijken zijn, stakingen, door overheden opgelegde verboden, oproer, extreme weersomstandigheden, dubbele netwerkstoringen (storing in secundaire én primaire voorzieningen) en indien de energievoorziening (w.o. aarding) of de klimaatbeheersing op de klantlocatie niet voldoet* […][16].
   Daarmee wordt een groot aantal scenario's mogelijk buiten de SLA-berekeningen gehouden. De verwachting van de klant komt daardoor mogelijk niet overeen met wat KPN daadwerkelijk aanbiedt.

[15] Zie verder paragraaf 3.1.2.5).
[16] Document: Bijlage MCTN dienstbeschrijving, versie 0.5, januari 2005.

De afdeling Zakelijke Markt heeft enig inzicht in welke klanten vitale belangen hebben bij de SDH-dienst. Er wordt onderscheid gemaakt tussen vier categorieën, op basis van de werkzaamheden van de klant. Het havenbedrijf zit bijvoorbeeld in categorie 3, ziekenhuizen in categorie 2 en de hulpdiensten in categorie 1. KPN heeft echter geen volledig inzicht in het doel waarvoor de klant de verbinding inzet. Bij herstel kan daarom ook geen rekening worden gehouden de wensen van klanten.

3.1.2.2 De afdeling Zakelijke Markt

De afdeling Zakelijke markt maakt interne afspraken met de afdeling Technisch Productmanagement (TPM) over de realisatie van diensten die aan klanten worden geleverd.

Werkwijze KPN

De afdeling TPM verzorgt het beheer en onderhoud van, onder andere, het SDH-netwerk. Er zijn meerdere diensten die gebruik maken van het SDH-netwerk en deze bieden hun klanten niet allemaal dezelfde afgesproken dienstenniveaus. In het beheer en de bewaking van het SDH-netwerk is echter niet direct zichtbaar voor welke dienst een SDH-verbinding wordt ingezet. TPM hanteert daarom één niveau van dienstverlening voor alle gebruikers van het SDH-netwerk. Het afgesproken beschikbaarheidsniveau is 98,8%. Voor de hersteltijd van storingen zijn geen afspraken gemaakt.

Bevindingen en analyse

Behalve de beschikbaarheid is ook de hersteltijd een belangrijk onderdeel van de Service Level Agreement met de klant en een onderscheidend verschil tussen de service levels Premium A en Premium B. In de interne SLA-afspraak tussen TPM en de commerciële afdelingen is echter niets opgenomen over hersteltijden. Ook hier is het dus onduidelijk hoe de aan de klant geboden garanties voor hersteltijd worden waargemaakt.

De categorie-indeling van klanten waarover de afdeling Zakelijke Markt beschikt, is niet automatisch beschikbaar voor TPM. De relatie tussen klant, de aard van het gebruik en de technische realisatie moet handmatig worden gelegd. In geval van storingen kan dan ook niet direct rekening worden gehouden met de prioriteit van de klant. Daarbij kan de mogelijke impact voor de klant ook niet goed worden ingeschat.

3.1.2.3 De afdeling Technisch Productmanagement en Network, IP & Access

De afdeling Netwerk, IP & Access (NIPA) heeft onderhoudscontracten met externe partijen. Leveranciers van apparatuur leveren ook onderhoudsdiensten, maar er zijn ook bedrijven die merk-onafhankelijke onderhoudsdiensten aanbieden.

Werkwijze KPN

NIPA heeft contracten met twee partijen voor onderhoud aan SDH-apparatuur. De eerste is Alcatel-Lucent, de leverancier van onder andere de DXC die het incident in de Waalhaven veroorzaakte. De tweede is Telmar, een internationaal bedrijf met een vestiging in Eindhoven, dat onder andere reparaties aan Alcatel-Lucent onderdelen verricht.

Bevindingen en analyse

Alcatel-Lucent heeft in 2008 aan KPN verzocht de oudere SDH-apparatuur uit dienst te nemen. De reden hiervoor is dat Alcatel-Lucent voorziet dat de onderdelen op een gegeven moment niet meer

beschikbaar zijn en dat de benodigde kennis over SDH in de tijd afneemt. Op verzoek van KPN is het onderhoudscontract echter verlengd tot 2015. Hoewel de onmiddellijke ondersteuning op grond van het contract niet afdwingbaar is, verloopt de samenwerking in de praktijk bijzonder goed. KPN laat de kennis op componentniveau volledig over aan Alcatel-Lucent.

3.1.2.4 Overige bevindingen

Er zijn tijdens het onderzoek geen documenten en/of bestanden aangetroffen waarin risico's (dreigingen, waarschijnlijkheden en mogelijke gevolgen) worden bijgehouden. Het risicomanagement is voor het SDH-netwerk enkel gericht op de vraag: kan KPN nog voldoen aan de Service Level Agreement? Dat leidt tot de vragen welk service level (en dus welke norm) gehanteerd wordt en hoe bepaald wordt of dat die norm gehaald is.

Er is geen norm aangetroffen die gebruikt wordt voor eenduidige risicobeoordeling. Het is aannemelijk dat iedere overeenkomst een eigen risico-opvatting met zich meebrengt en dat de SLA met de klant belangrijker is dan de interne KPN – SLA's.

Afgezien van de beheersmaatregelen die getroffen zijn onder het Life Cycle Management, heeft het agentschap geen aanvullende risicobeheersmaatregelen aangetroffen[17].

Een mogelijkheid zou zijn geweest om vitale verbindingen te spreiden over DXC's, zodat bij uitval van één DXC de impact beperkt zou zijn. KPN heeft daar echter niet voor gekozen.

KPN geeft aan terughoudend te zijn met het aan klanten melden van aantallen gebruikte onderhoudsperiodes en de aard en omvang van het gepleegde onderhoud, omdat dit volgens KPN de klant mogelijk onnodig ongerust maakt.

Opmerkelijk is verder dat KPN geen uitgewerkt calamiteitenplan heeft voor een grootschalige uitval als tijdens het Waalhaven incident. KPN kent wel een procedure voor calamiteiten onder de naam *Be Alert*. Deze procedure biedt structuur aan de bestrijding en op- en afschaling van incidenten, maar specifieke voorbereidende activiteiten zijn niet waargenomen. *Be Alert* bestaat uit 5 niveaus met bijbehorende kleuren. Het laagste niveau (Code Groen) representeert een normale, stabiele toestand, zonder verstoringen. Aan de overige niveaus zijn, in oplopende volgorde, de Code Blauw, Geel, Oranje en Rood toegekend. Elk niveau kent een aparte procesbeschrijving waarin staat wie de leiding heeft en welke acties er genomen moeten worden.

3.1.2.5 Hogere waakzaamheid voor vitale verbindingen

KPN heeft met IVENT, de bedrijfsgroep Informatievoorziening en –Technologie van het ministerie van Defensie, aanvullende afspraken gemaakt over de dienstverlening voor verbindingen ten behoeve van C2000. Deze zijn vastgelegd in het Document Afspraken en Procedures (DAP). Dit document beschrijft aanvullende afspraken over incidentmelding en –afhandeling, wijzigingsbeheer, gepland onderhoud en rapportage, maar overstijgt nergens de SLA-afspraken over beschikbaarheid en hersteltijden. Zo is bijvoorbeeld afgesproken dat KPN IVENT informeert bij werkzaamheden die een onderbreking kunnen veroorzaken van meer dan 50 milliseconden. Ook kan IVENT gepland onderhoud weigeren wanneer zij meent dat onderbrekingen van de dienst op dat moment zeer ongewenst zijn. Verder is er maandelijks overleg tussen KPN, IVENT en de gebruikers van C2000. Ook is er planning over evenementen zoals risicowedstrijden en muziek

[17] Voor C2000 zijn wel aanvullende beheermaatregelen getroffen. Zie hiervoor paragraaf 3.1.2.5

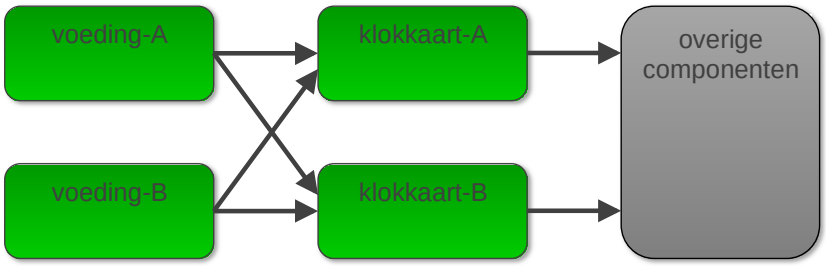
festivals die in een jaarkalender worden gehouden. Bij noodsituaties (GRIP 3 en hoger) is een liaison persoon van KPN aanwezig bij het LOCC. Ook neemt KPN deel aan diverse rampenoefeningen op het terrein van openbare orde en veiligheid en oefeningen van het ministerie van Defensie. Daarnaast is KPN betrokken bij het opstellen van draaiboeken en evaluaties en zijn er aparte uitwijkprocedures, die periodiek worden getest.

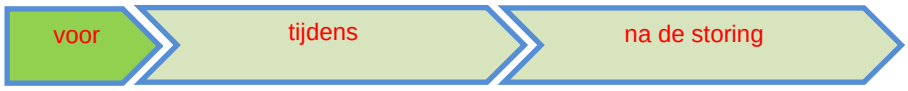
3.2 Oorzaak en aanpak van de storing

In de nacht van 26 op 27 juli 2011 pleegt KPN onderhoud aan een DXC in de Waalhaven te Rotterdam. Tijdens dit onderhoud treedt een zware technische storing op. Ongeveer 6200 transmissie verbindingen, waaronder 86 C2000 verbindingen, zijn gedurende bijna zeven uur verstoord. In deze paragraaf worden de gebeurtenissen in de aanloop naar het incident en de afwikkeling ervan, beschreven.

Bij deze beschrijving staat telkens een schematisch overzicht van de toestand van de belangrijkste componenten van de DXC die deel uitmaakte van de storing: de voedingen en de klokkaarten. Kleuren geven de werking van een component weer: groen betekent dat de component correct werkt, geel betekent een verminderde werking en rood betekent dat de component geheel is uitgevallen. Pijltjes geven aan of een voeding spanning levert, of dat een klokkaart een kloksignaal afgeeft.

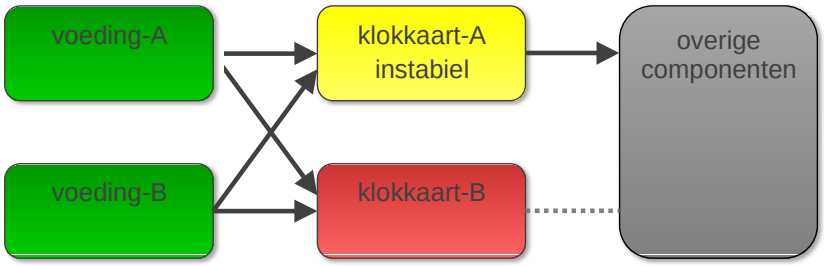
Onderstaande figuur geeft de uitgangstoestand aan; alle componenten functioneren normaal.





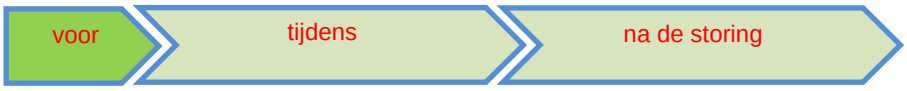
5 juni 2011, overdag

Oorzaak
Op 5 juni 2011 constateert KPN voor het eerst een probleem met de DXC. Het telecommunicatie-verkeer over deze DXC vertoont enige onderbrekingen van enkele seconden tot minuten en veroorzaakt een groot aantal klokkaartalarmen. Doordat apparatuur in de DXC dubbel is uitgevoerd, hebben de onderbrekingen dat op dit moment geen grote impact op de dienstverlening. Alcatel Lucent, die voor dit apparaat de leverancier en onderhoudspartner is, constateert op afstand dat klokkaart-B geen signaal levert en dat klokkaart-A alarmen veroorzaakt.



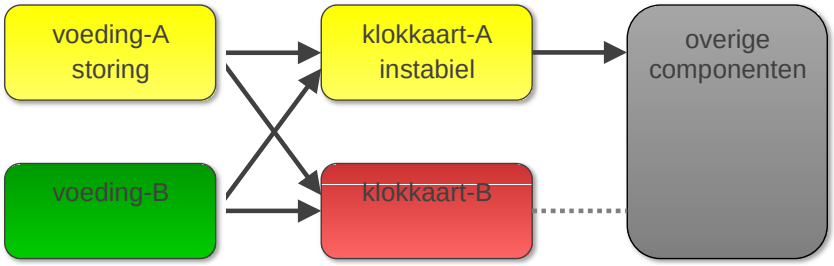
Aanpak
Omdat de situatie stabiel is komen Alcatel-Lucent en KPN overeen op 6 juni verder onderhoud uit te voeren.

Bevindingen en analyse
De alarmering en bewaking van de status van de DXC functioneren naar behoren. Ook de ondersteuning door de onderhoudspartner is volgens verwachting.



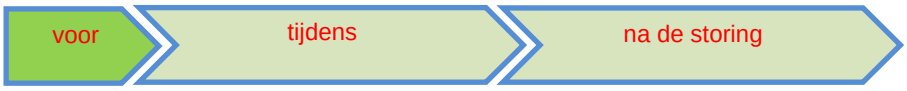
6–7 juni 2011, onderhoudsperiode

Oorzaak
In de ochtend van 6 juni wordt voor het eerst geconstateerd dat de schakelaar op voeding-A op 'aan' staat, maar dat desondanks het controle–lampje niet brandt. Er is geen automatisch alarm afgegeven voor deze voeding. Op dit moment is onduidelijk wat er precies aan de hand is met voeding–A. Wel is helder dat voeding-A onbetrouwbaar is. Voeding-B functioneert normaal.
In de nacht van 6 op 7 juni 2011 zijn KPN en Alcatel-Lucent ter plaatse. Metingen door Alcatel-Lucent bevestigen de bevindingen van vorige dag: klokkaart-B levert geen signaal en klokkaart-A is instabiel, hetgeen invloed heeft op de verkeersafwikkeling. Drie van vier belangrijkste onderdelen functioneren niet zoals het hoort.



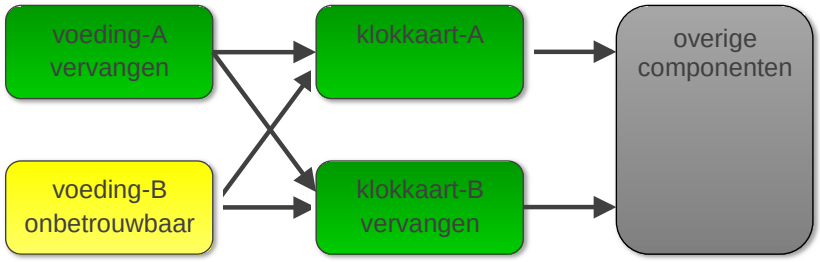
Aanpak
Alcatel-Lucent adviseert om beide klokkaarten te vervangen en voert deze vervanging uit. Dit is een beproefde procedure. Als voorbereiding op het onderhoud zijn volgens het protocol van alle vitale onderdelen twee stuks reserve aanwezig. Gedurende de actie blijkt een van de benodigde klokkabels defect te zijn.
De defecte voeding-A wordt vervangen. Daarmee wordt klokkaart-A stabiel en verdwijnen de problemen met de verbindingen.
Klokkaart-B wordt alsnog vervangen en functioneert. Van onmiddellijke vervanging van klokkaart-A, zoals de vervangingsprocedure van KPN voorschrijft, wordt afgezien omdat deze nu normaal lijkt te functioneren.

Bevindingen en analyse
KPN heeft in de door Alcatel-Lucent geleverde DXC's destijds niet gekozen voor de optie om via een alarmsysteem te detecteren of een van de voedingen onderbroken is. Wel heeft KPN in 2002 een wijzigingsverzoek ingediend om alsnog voedingbewaking te realiseren. Alcatel-Lucent heeft deze wijziging in een operationele DXC destijds ten stelligste afgeraden. Dit zou zeker leiden tot storingen en verkeersonderbrekingen. De consequentie hiervan is dat de bewaking van voedingen door KPN periodiek op locatie moet plaatsvinden.
De dubbele uitvoering van de DXC zorgt ervoor dat ondanks een onbetrouwbare voeding impact voor klanten uitblijft, maar 'maskeert' zo het defect, waardoor de DXC nog zonder voedings-problemen lijkt te functioneren. De speelruimte is dan echter wel opgebruikt, zodat een eventueel volgende uitval direct voor klantimpact kan zorgen.



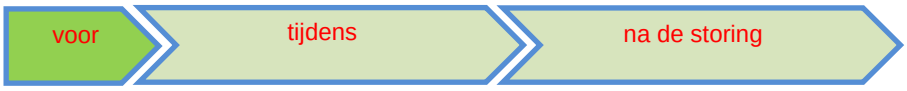
6–7 juni 2011, onderhoudsperiode (vervolg)

Oorzaak
Alcatel-Lucent constateert op afstand dat de (niet-vervangen) voeding-B de klokkaart-A van onbetrouwbare voeding voorziet en trekt de conclusie dat de niet-vervangen voeding-B preventief vervangen moet worden. Klokkaart-A loopt alleen stabiel als deze wordt gevoed door voeding-A. Een tweede onderhoudsactiviteit wordt ingepland om de voeding-B te vervangen.



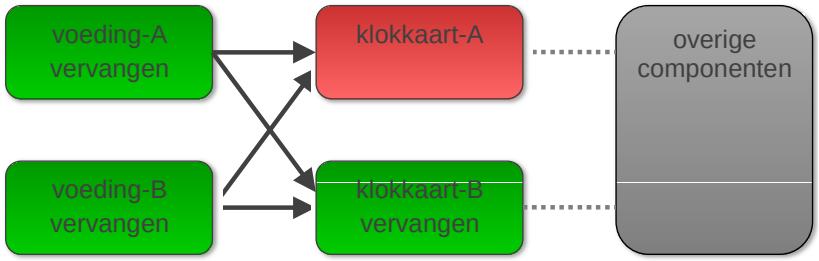
Aanpak
De uitgevallen componenten zijn later aan een nader onderzoek onderworpen. Zij blijken echter probleemloos te functioneren op een DXC testopstelling. Alcatel-Lucent en KPN kunnen dat niet verklaren en verrichten nader onderzoek. Om de vervanging goed voor te bereiden, wordt de actie bovendien geoefend in een laboratorium van Alcatel-Lucent en op een andere DXC van KPN. Dit verklaart de lange periode tussen 7 juni en 27 juli, het moment waarop voeding-B uiteindelijk vervangen zal worden.

Bevindingen en analyse
In een testopstelling functioneerden de componenten probleemloos. Dat is een aanwijzing dat de componenten klaarblijkelijk soms wel en soms niet goed functioneren, afhankelijk van omgevingsfactoren. Een technisch onderzoek naar mogelijke omgevingsfactoren is echter niet uitgevoerd.



27 juli 2011, onderhoudsperiode

Oorzaak
Alcatel-Lucent en KPN starten 's nachts omstreeks 00:30 uur met het vervangen van voeding-B. Bij het uitnemen van de voeding valt onverwacht klokkaart-A uit. Dat is de directe aanleiding voor de verstoring. Ondanks dat klokkaart-A uitvalt, komt er geen signaal naar de passieve klokkaart-B om de klokfunctie over te nemen. Er is in de DXC dus een normaal functionerende voeding-A en een normaal functionerende klokkaart-B, hetgeen voldoende zou moeten zijn voor een ongestoord functioneren, maar ondanks dat is er toch een verstoring. Beide onderdelen zijn overigens in de nacht van 6 op 7 juni geplaatst. Ondertussen vervangt KPN met behulp van Alcatel-Lucent voeding-B.

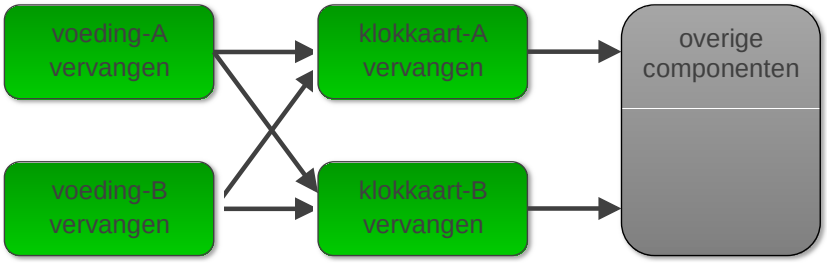


Aanpak
Op het moment dat op 27 juli 2011 aan het preventief onderhoud wordt begonnen is in ieder geval een expert van Alcatel-Lucent aanwezig en een tweedelijnsspecialist van KPN. Onduidelijk is of ook nog een of meer inhoudelijke medewerkers van de uitvoerende afdeling ter plaatse zijn. Dit blijkt ook niet meer te achterhalen.
De verstoring was mogelijk te voorkomen geweest als vóór de preventieve vervanging van de voeding-B eerst klokkaart-A vervangen zou zijn. Daarmee zou de oorspronkelijke vervangings-procedure van twee klokkaarten op 6 juni 2011 alsnog zijn afgerond. Toen op 7 juni 2011 werd besloten om klokkaart-A niet te vervangen, was bij Alcatel-Lucent nog niet bekend dat klokkaart-A defect is. De instabiliteit van klokkaart-A wordt dan nog aan de voeding toegeschreven. Met de vervangen voeding wordt klokkaart-A immers stabiel; het probleem met de klokkaart lijkt opgelost.

Bevindingen en analyse
De verstoring ontstaat omdat de normaal functionerende maar niet actieve klokkaart-B 'niet wordt bereikt' om het werk van de instabiele klokkaart-A over te nemen. Het gevolg is dat de matrix, het verkeersplein dat al het verkeer routeert, instabiele kloksignalen krijgt. Om het telecommunicatie-verkeer te kunnen routeren is een stabiel kloksignaal echter essentieel. Door het instabiele kloksignaal van klokkaart-A kan de matrix het verkeer niet meer verwerken. Daardoor vallen de verbindingen uit en ontstaat het incident. Klanten ervaren uitval van het telecommunicatieverkeer. Het onderhoud op de ene voeding wordt verondersteld zonder impact uitgevoerd te kunnen worden door de beschikbaarheid van de andere voeding. Deze aanname blijkt niet juist te zijn. KPN gaat er van uit dat bij deze vervanging geen sprake zal zijn van klantimpact. Daarom worden de klanten niet vooraf van het onderhoud op de hoogte gebracht.

27 juli 2011, onderhoudsperiode (vervolg)

Oorzaak
KPN laat zich vervolgens adviseren door Alcatel-Lucent's *last support,* het Technical Excellence Center (hierna: TEC ALU) in Stuttgart. Het advies van TEC ALU is om de DXC zichzelf te laten herstellen.
Om 02:15 uur neemt KPN het besluit tot zelfherstel. Dit herstel vindt echter onvoldoende plaats: er komen zeer traag en onvolledig weer verbindingen op. De kloktijden van het verkeersplein en beide klokkaarten komen niet tot een synchroon signaal. Ongeveer 1.000 tot 3.000 verbindingen zijn hierdoor verbroken.
Op advies van TEC ALU besluit KPN om 03:45 uur tot een ingrijpende 'koude herstart'. Dit is een volledige herstart, waarbij alle verbindingen (circa 6200) worden verbroken. Vervolgens bouwt de DXC al het verkeer op basis van een nieuw synchroon kloksignaal opnieuw op.
Voordat Alcatel-Lucent aanvangt met de 'koude herstart' wordt klokkaart-A vervangen.
De 'koude herstart' heeft het beoogde resultaat. Om 06:50 uur is het herstel van de verbindingen voltooid, op een paar uitzonderingen na. Omstreeks 10:00 uur in de ochtend van 27 juli 2011 zijn alle diensten weer hersteld.



Aanpak
Ongeveer vijftig minuten na het ontstaan van het incident start KPN de calamiteitenprocedure *Be Alert* op (zie 3.1.2.4). Drie kwartier later wordt code Geel ingeschakeld, als op last van het derdelijns support van TEC ALU te Stuttgart wordt geadviseerd om de DXC zichzelf te laten herstellen.
Vier uur na het ontstaan van het incident wordt *Be Alert* code Oranje van kracht, waarna KPN haar communicatieteam informeert. De verantwoordelijke manager vraagt assistentie voor het bepalen van de impact.
Als de 'koude herstart' is voltooid communiceert KPN met klanten (of probeert dat) om verbindingen te controleren en om op de diverse klantlocaties herstelwerkzaamheden uit te voeren.
Het dienstenmanagement is buiten kantoortijd niet ingericht om dergelijke calamiteiten in behandeling te nemen. Daardoor is de voortgang minder dan vereist. Bovendien zijn de communicatieprocedures onvoldoende uitgewerkt of onbekend bij sommige medewerkers van KPN.
Als om 10:00 uur alle diensten weer zijn hersteld, blijft de stabiliteit van de diensten extra bewaakt. Ook wordt actie ondernomen om alarmen van de DXC prominent zichtbaar te maken op het Netwerk Operator Center.
Tussen de verschillende afdelingen van KPN bestaat geen eenduidig beeld wanneer gepland onderhoud wel en wanneer niet aan de klant wordt gemeld, zo blijkt uit verschillende interviews. Tussen het segment Zakelijke Markt en Technisch Productmanagement bestaat een verschillend beeld. Er is, naast een formeel communicatiekanaal via de Regiekamer, ook een informeel communicatiekanaal in gebruik, via de Business Service Desk. Uit de interviews blijkt: 'KPN maakt een afweging wat zij klanten meedeelt inzake onderhoud dat geen impact zou mogen hebben op de

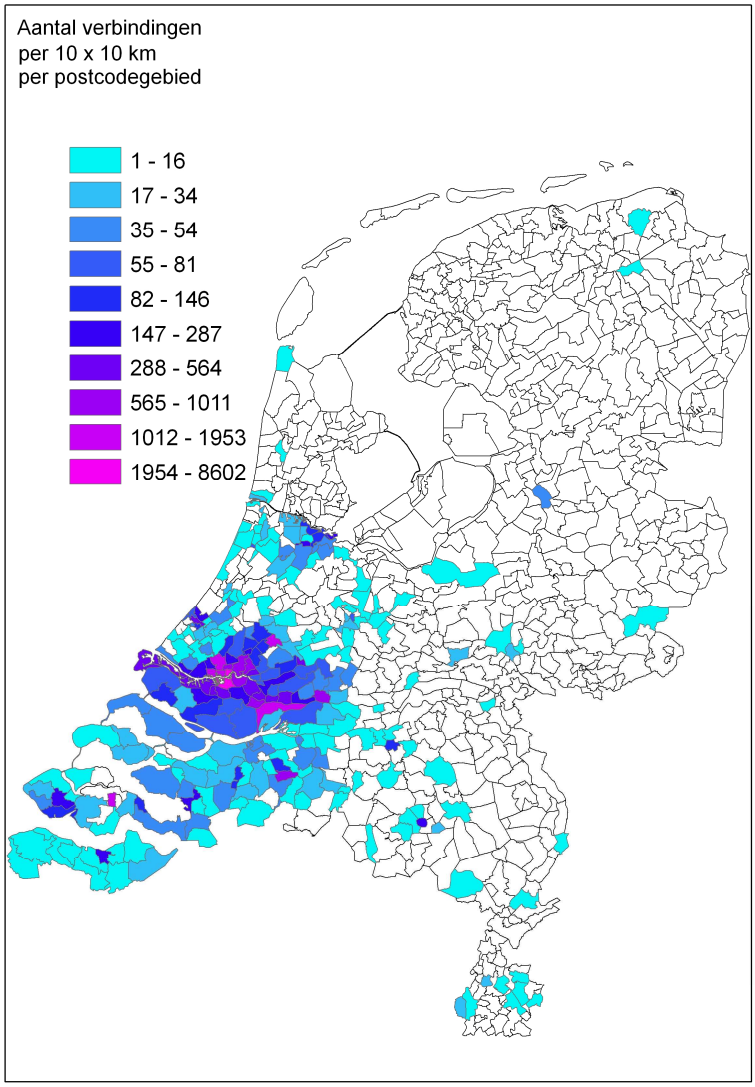
dienstverlening. Als bijvoorbeeld iets redundant is ingericht, dan merkt de klant er niets van'. en 'Je kunt alles communiceren, maar dan krijgt een klant onnodig de indruk dat er veel onderhoud plaatsvindt omdat een dienst uit veel componenten bestaat. Dit is dus ter voorkoming van ongerustheid'. Uitspraken van vergelijkbare strekking zijn terug te vinden in meerdere interviews.
De klant IVENT, afnemer van onder andere de verbindingen voor C2000, heeft naast de SLA aanvullende afspraken met KPN gemaakt over de communicatie in geval van (gepland) onderhoud. In het Document Afspraken en Procedures van 14 april 2010 tussen IVENT en KPN is afgesproken dat werkzaamheden die een onderbreking van 50 milliseconden of langer *kunnen* veroorzaken door KPN moeten worden gemeld. Het geplande onderhoud van 26 op 27 juli 2011 zou een dergelijke uitval inderdaad kunnen veroorzaken. Het onderhoud is echter niet gemeld volgens de afspraken, omdat de aanname van KPN voorafgaand aan het onderhoud is dat de klantimpact nihil zal zijn. Het betreffende onderhoud is echter wel buiten de formele procedure om door KPN aan IVENT gemeld.

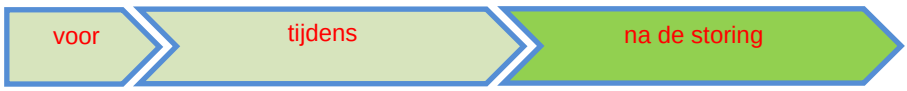
Bevindingen en analyse
Met de vervanging van klokkaart-A zijn zowel beide voedingen als beide klokkaarten vervangen. Niet duidelijk is wat de herkomst is van de geplaatste onderdelen. Aannemelijk is dat dit reserveonderdelen zijn uit eerder ontmantelde DXC's.
Er is niet voorzien in het scenario waarin de DXC ook na de 'koude herstart' niet zou functioneren en dus volledig zou uitvallen; een noodscenario ontbrak.
Uit verscheidene bronnen blijkt dat het voor KPN bovendien niet eenvoudig is om snel een betrouwbare lijst samen te stellen van klanten die getroffen zijn door een verstoring. Hierdoor bestond ook geen goed inzicht in, of inschatting van, de impact die de verstoring op klanten zou hebben. KPN geeft bovendien aan dat niet wordt geregistreerd voor welke doeleinden de klanten verbindingen afnemen. Het is wel bekend wat de impact voor C2000 is, maar niet direct wat de betekenis is voor bijvoorbeeld het Rotterdamse openbaar-vervoerbedrijf RET.
Door de storing zijn uiteindelijk ongeveer 6200 verbindingen van 2Mb getroffen. Eén 2Mb verbinding kan meerdere klantverbindingen bevatten. De klantimpact is dus groter. Van de getroffen verbindingen zijn er 86 in gebruik voor C2000. Welke dat waren, is niet direct duidelijk; pas een aantal dagen later zijn de juiste lijnen van C2000 in beeld.
Niet alle verbindingen zijn overigens gelijktijdig uitgevallen. Tijdens het begin van de storing ligt het aantal op een percentage 15% tot 50% (code Geel in de *Be Alert* calamiteitenprocedure). Pas tijdens de 'koude herstart' stijgt het aantal getroffen verbindingen naar 100% (code Oranje).

Geografische impact

De impact van het incident bestrijkt een groot geografisch gebied; er zijn zelfs verbindingen getroffen in Groningen en Limburg. Er is niet onderzocht welke eindgebruikers hinder hebben ondervonden van de verstoring, maar dat men hinder heeft ondervonden is bekend. Het is aannemelijk dat de afnemers van verbindingen buiten Rotterdam-Rijnmond eventuele uitval niet in verband hebben gebracht met het Waalhaven incident, aangezien er in de media niets over verstoringen op grote afstand van Rotterdam gemeld is.

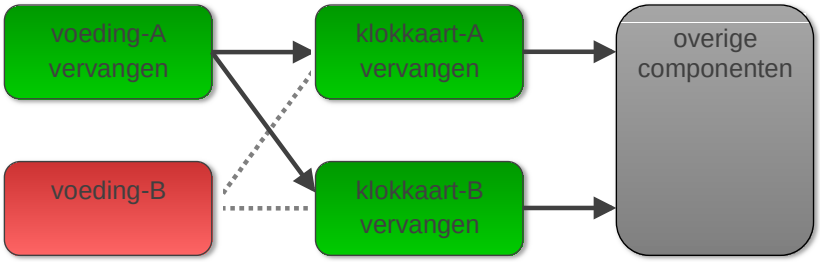
De analyses zijn gemaakt op basis van de postcode van alle verbindingen, op 3 cijfers nauwkeurig. Per postcodegebied is het aantal verbindingen geteld waarvan een melding beschikbaar was.





27 juli 2011, 's avonds

Oorzaak
Sinds het herstel van de verbindingen na de 'koude herstart' werkt gedurende de hele dag de DXC naar behoren. Het incident lijkt opgelost. Omstreeks 22.00 uur doet zich echter onverwacht opnieuw een probleem voor: voeding-B schakelt zichzelf uit. Omdat voeding-A nog functioneert, worden noch het verbindingsverkeer noch de kloksignalen van de klokkaarten hierdoor beïnvloed. De acute fase van het incident eindigt hier en de nafase begint.

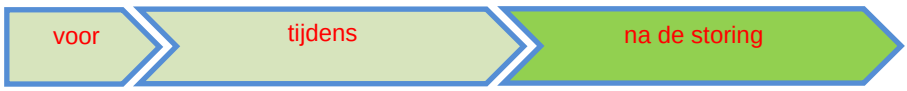


Aanpak
Reparatie wordt te risicovol geacht en zal alleen worden gedaan bij spontane uitval. De getroffen DXC staat wel onder een verscherpt controleregime. Om het herstel te voltooien stelt KPN drie werkstromen op.

Werkstroom 1: Het stabiliseren van de DXC en het met spoed overplaatsen van geprioriteerde klanten van deze DXC naar diverse andere SDH-routes. Het doel is om zoveel mogelijk kritieke verbindingen van de getroffen DXC weg te halen.
Werkstroom 2: Als KPN de meest kritieke lijnen heeft verplaatst naar aan andere DXC van een nieuwere generatie, volgt verplaatsing van de overige verbindingen om de getroffen DXC volledig vrij te maken.
Werkstroom 3: Zodra de getroffen DXC is vrijgemaakt laat KPN een onderzoek uitvoeren naar de oorzaak van de verstoring.

Op 1 augustus 2011 worden bijzondere procedures afgekondigd voor al het werk aan DXC's in het SDH-netwerk. Op 4 augustus worden deze gedeeltelijk versoepeld.

Bevindingen en analyse
Alcatel-Lucent en KPN kunnen geen adequate verklaring geven voor deze nieuwe uitval. Daarom wordt besloten tot het uitvoeren van een *Root Cause Analysis (RCA)*, een grondig onderzoek naar de achterliggende oorzaak van de problemen met deze DXC. De getroffen DXC moet vrijgemaakt zijn voordat dit onderzoek kan worden uitgevoerd.



27 juli – december 2011, nafase

Oorzaak
Op 7 augustus is de verplaatsing van de verbindingen van C2000, het Rotterdamse openbaar-vervoerbedrijf RET, Havenbedrijf Rotterdam en Rotterdam The Hague Airport gereed(werkstroom 1). Vervolgens worden alle overige klanten overgezet naar een andere DXC. Deze werkzaamheden zijn op 22 augustus afgerond (werkstroom 2). De DXC is daarmee volledig losgemaakt van het SDH-netwerk. KPN stuurt de DXC op naar de Verenigde Staten, waar het bedrijf Bell Labs de RCA uitvoert. Het eindrapport van dit onderzoek is op 24 november gereed (werkstroom 3).

Aanpak
In drie weken tijd, van 29 juli 2011 tot en met 22 augustus 2011, heeft het projectteam de DXC vrijgemaakt door verbindingen fysiek om te zetten naar een DXC van de nieuwe generatie. De migratie naar een andere DXC is risicovol. Er zijn dan ook restricties op het uitvoeren van werkzaamheden aan DXC's in het algemeen en zelfs aan daaraan verbonden kabels afgekondigd. De migratie verloopt uiteindelijk goed, behoudens een incident door verkeerde labeling. De migratie heeft zoals voorzien tot meerdere korte onderbrekingen van alle verbindingen geleid.
Op 21 december 2011 plaatst KPN een bericht op de nieuwspagina[18], waarin wordt aangegeven wat de oorzaak was van de storing en welke acties worden ondernomen (zie kader).

Vervanging onderdelen
Cross connects staan bekend als zeer robuuste en betrouwbare systemen. Dit type storing had nog niet eerder plaatsgevonden. Nu de oorzaak bekend is, wil KPN voorkomen dat deze situatie zich nogmaals kan voordoen. Daarom wordt in alle 88 cross connects van KPN de zwakke component in de klokkaarten vervangen. De vervanging zal vanaf begin 2012 starten en zal deel uitmaken van de reguliere onderhoudswerkzaamheden. Dat betekent dat klanten er in principe geen overlast van zullen ondervinden.

Passage uit het bericht op de nieuwspagnia van KPN (KPN News stream, 21 december 2011).

Bevindingen en analyse
Opmerkelijk is dat op 29 juli 2011 nog niet bekend is welke andere dan de meest vitale verbindingen zijn getroffen. Het complete beeld wordt op 1 augustus verwacht.
Opmerkelijk is ook het grote tijdsbeslag dat het uitzoeken van klantimpact heeft gelegd. In geval van een calamiteit met totaaluitval van een DXC kan migratie leiden tot uitval van diensten gedurende drie weken.
Het RCA onderzoek wijst de oscillator van klokkaart-A aan als meest waarschijnlijke oorzaak. De oscillator werkt wel, maar heeft meer elektrisch vermogen nodig dan normaal. In de situatie waarbij beide klokkaarten correct functioneren en slechts één voeding beschikbaar is, draait de voeding op ongeveer 90 procent van zijn maximale capaciteit. Wanneer echter een van de

[18] http://forum.kpn.com/t5/News-stream/Technische-oorzaak-KPN-storing-Rotterdam-in-juli-bekend/ba-p/9797

klokkaarten meer vermogen nodig heeft, wordt meer vermogen van de voeding gevraagd dan deze kan leveren. Bij het verwijderen van voeding-B op 27 juli krijgt de oscillator op klokkaart-A daardoor te weinig stroom en valt uit.
Het juiste functioneren van de oscillator is niet op afstand te controleren. De DXC apparatuur is van een bouwjaar dat monitoring op componentniveau nog niet gangbaar is. Het is op een later moment ook niet meer in te bouwen. Dat geldt zeker als de leverancier geen (software)updates meer verleent als gevolg van het afkondigen van een 'end of service' deadline.
Het routeren van het telecommunicatieverkeer gaat mis door het afwijkende kloksignaal. Normaal gesproken moet een haperende klokkaart omschakelen naar de passieve klokkaart. Dit proces duurde te lang. Als de slecht functionerende oscillator helemaal kapot was geweest, dan zou de overschakeling waarschijnlijk wel zijn gelukt.
In de RCA beschrijft Bell Labs bovendien dat er dunne koperdraden en een losse moer aangetroffen zijn in en op de DXC. De koperdraden zijn het gevolg van het ontmantelen en verwerken van coaxkabels in de ruimte waarin de DXC zich bevindt. De RCA beschrijft een scenario waarbij de dunne koperdraden al in juni 2011 kortsluiting kunnen hebben veroorzaakt, waardoor de overspanningsbeveiliging van de voeding in werking is getreden. Vervolgens zou op 27 juli, na het herstel door de 'koude herstart' nogmaals een koperdraadje op een plek zijn gevallen, waardoor opnieuw een voeding zou zijn uitgevallen.
Theoretisch is dit kortsluitingscenario inderdaad mogelijk. Dit is echter niet onomstotelijk aangetoond en theoretisch is er maar een heel kleine kans dat tweemaal in twee maanden een gevallen stukje koperdraad zorgt voor uitval van een voeding. Duidelijk is wel dat dergelijke vervuiling risicoverhogend en vermijdbaar is.

3.3 Maatschappelijke effecten van de uitval

In deze paragraaf komt aan de orde wat maatschappelijke effecten waren van de KPN-storing in de nacht van 26 op 27 juli 2012. Het onderzoek heeft zich hierbij gericht op de vitale organisaties die direct hinder en overlast hebben ondervonden.

Om een goed beeld te krijgen van gevolgen van de storing voor de vitale sectoren heeft de Inspectie VenJ bij KPN een lijst opgevraagd met alle aangesloten lijnen op de cross- connect in de Waalhaven. Het betreft in totaal circa 6200 aansluitingen. Een nadere analyse wijst uit dat veel bedrijven, instellingen en organisaties in vrijwel alle vitale sectoren te maken hebben gehad met deze storing.

Het tijdstip waarop de storing plaatsvond, in de nachtelijke uren, maakte dat veel van de getroffen verbindingen 'slapend' waren. Daardoor is de uitval vaak niet opgemerkt. Ook kan de Inspectie in veel gevallen niet vaststellen waarvoor de aangeslotenen de betreffende lijnen gebruiken. Een aanzienlijk deel daarvan betreft vrijwel zeker 'normale' telefonieverbindingen. Mede gezien het moment van de storing is de impact op het functioneren van het betreffende bedrijf, instelling of organisatie waarschijnlijk gering geweest. Daar komt bij dat sommige lijnen slechts enkele malen per etmaal worden gebruikt om data te versturen. Als dit niet in de storingsperiode het geval was, heeft het betreffende bedrijf of organisatie hiervan ook niets gemerkt.

3.3.1 Uitgevallen verbindingen en voorzieningen

De uitval van de cross connect in Rotterdam had een aantal direct merkbare maatschappelijke effecten. Dit betrof de uitval van verbindingen via het C2000-communicatienetwerk voor de hulpdiensten, de uitval van het P2000-netwerk voor alarmering van deze diensten, het onbruikbaar worden van lijnen waarmee bedrijven en instellingen rechtstreeks verbonden zijn met de meldkamer van hulpdiensten (waaronder ook brandmeldinstallaties in gebouwen), uitval van (delen van) het Nationaal Noodnet, uitval van communicatievoorzieningen in het metronetwerk van Rotterdam en een aantal kleinere effecten. Hieronder volgt een overzicht van de uitgevallen verbindingen en voorzieningen.

C2000
Er was geen mobilofoonverkeer meer mogelijk tussen de regionale meldkamers en eenheden van politie, brandweer en ambulancediensten in (delen van) de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid en Hollands Midden. Het onderlinge portofoonverkeer tussen de eenheden (de 'direct-mode') bleef wel intact, maar was - gezien de beperkte reikwijdte van deze verbindingen - geen afdoend alternatief voor het mobilofoonverkeer.

P2000
Er was geen mogelijkheid om brandweerpersoneel te alarmeren voor (spoedeisende) uitrukken. Telefonisch alarmeren vergde aanzienlijk meer tijd, terwijl delen van het vaste en mobiele telefoonnetnetwerk ook ernstige hinder van de storing ondervonden. De mogelijkheid tot alarmering van de brandweer was daarmee sterk gereduceerd.

Directe lijnen van brandmeldinstallaties
De mogelijkheid om brandmeldingen automatisch door te geven was weggevallen, terwijl die verwachting wel bestaat. Brandmeldingen moesten - waar mogelijk door aanwezig personeel – via normale telefoonverbindingen worden doorgegeven, waardoor sprake was van langere alarmeringstijden. Delen van het vaste en mobiele telefoonnetwerk gaven eveneens een storingsindicatie te zien.

Directe lijnen tussen de meldkamers van de hulpdiensten en bedrijven en instellingen
In de veiligheidsregio's Rotterdam-Rijnmond, Zuid-Holland Zuid, Hollands Midden en Zeeland (beperkt) vielen verbindingen van tijd tot tijd uit. Zo was er soms geen directe verbinding mogelijk tussen de meldkamer, de ambulancedienst en ziekenhuizen en bleken de directe lijnen tussen chemische bedrijven en de meldkamer niet (altijd) te functioneren.

Nationaal Noodnet
Dit netwerk dient als achtervang als de normale communicatieverbindingen (door welke oorzaak dan ook) uitvallen. Deze achtervang bleek (in delen van de betrokken regio's) ook niet meer bruikbaar.

Communicatievoorzieningen in het metronetwerk
Doordat geen mobilofoonverbinding meer mogelijk bleek met de metrobestuurders heeft de RET het metronetwerk stilgelegd (niet opgestart).

3.3.2 Bevindingen

De Inspectie VenJ heeft het onderzoek specifiek gericht op de bedrijven, instellingen en organisaties waarvan direct duidelijk was dat de storing een grote impact had of waarvan bleek dat zij direct met de storing zijn geconfronteerd. Daarnaast is contact gelegd met de bedrijven en organisaties uit de vitale sectoren 'waterlevering' en 'waterbeheer' om vast te stellen in hoeverre zij daadwerkelijk hinder van de storing hebben ondervonden. De sector 'energielevering' is niet in het onderzoek betrokken, omdat direct duidelijk was dat de energielevering niet onderbroken is geweest.

Ook heeft de Inspectie VenJ gesproken met de organisaties die rechtstreeks geconfronteerd zijn met uitval van communicatievoorzieningen. Het gaat hierbij om de betrokken veiligheidsregio's, de RET en Luchtverkeersleiding Nederland. Ook is contact gezocht met partijen waarvan het vermoeden bestaat dat zij met uitval geconfronteerd zijn of waarvan in de media melding is gemaakt. Dit zijn het Havenbedrijf Rotterdam, de luchthaven Rotterdam-The Hague Airport, de drinkwaterleidingbedrijven Evides en Oasen, het Hoogheemraadschap van Schieland en de Krimpenerwaard en het waterschap Hollandse Delta.

Aan de bij het onderzoek betrokken organisaties is gevraagd met welke uitval van communicatievoorzieningen zij zijn geconfronteerd en welke maatregelen zij hebben getroffen om de maatschappelijke effecten te minimaliseren. Ook is onderzocht of deze maatregelen ad hoc zijn genomen of dat het maatregelen betreft die zijn voorbereid in plannen. Daarnaast is aan de betrokken organisaties gevraagd met welke bijzonderheden zij bij de afhandeling van dit incident verder nog zijn geconfronteerd.

Veiligheidsregio Rotterdam-Rijnmond

In de Veiligheidsregio Rotterdam-Rijnmond vielen C2000 en P2000 uit, alsmede de directe verbinding tussen de meldkamer en het netwerk voor de CIN-meldingen[19] en de directe verbinding met de ziekenhuizen. Vanaf het begin van de storing tot ongeveer 04:00 uur bleken sommige verbindingen soms wel te functioneren, maar na de 'koude herstart' van de DXC viel alles opnieuw uit.

De veiligheidsregio schaalde aanvankelijk op naar GRIP 2. Omdat KPN aangaf dat de storing naar verwachting rond 03:00 uur weer zou zijn verholpen, is slechts een beperkt aantal maatregelen genomen om de bereikbaarheid van eenheden mogelijk te maken. In de veiligheidsregio was mobiel telefoonverkeer (via een andere provider dan KPN) nog wel mogelijk, zodat eenheden (beperkt) bereikbaar waren.
De veiligheidsregio heeft de draaiboeken voor de millenniumwisseling geraadpleegd om daaruit maatregelen te destilleren die ook in deze situatie gebruikt konden worden. De veiligheidsregio heeft KPN verzocht een liaison voor het Regionaal Operationeel Team (ROT) beschikbaar te stellen. Dit is ook gebeurd, maar de liaison kon weinig feitelijk benodigde informatie verschaffen.
Omdat na de koude herstart van de DXC om 04:00 uur opnieuw sprake was van uitval, heeft de veiligheidsregio rond 07:00 uur opgeschaald naar GRIP 4. De storing betrof op dat moment meerdere gemeenten en het was onduidelijk hoe de exacte omvang van de storing zich zou manifesteren bij het 'ontwaken' van de stad. De veiligheidsregio beëindigde GRIP 4 rond 09:00 uur.

De veiligheidsregio verwondert zich over het gegeven dat KPN geen informatie kon verschaffen over de te verwachten omvang van de storing. Er was die nacht geen overzicht beschikbaar van de aansluitingen op de betreffende DXC, noch van de soorten verbindingen die daaraan waren verbonden. Daardoor kon het Regionaal Operationeel Team (ROT) niet vanuit de te verwachten scenario's maatregelen voorbereiden.
Ook vindt de veiligheidsregio het ongewenst dat KPN geen uitsluitsel kon geven over de te verwachten tijdsduur van de uitval. In eerste instantie verwachtte KPN dat de storing twee-en-een-half uur (tot 03:00 uur) zou duren. Na drie-en-een-half uur (om 04:00 uur) voerde KPN een 'koude herstart' van de DXC uit. Dit had tot gevolg dat alle verbindingen geheel uitvielen. Op dat moment was KPN niet in staat aan de veiligheidsregio aan te geven hoe lang deze (grotere) storing zou duren. Daar komt nog bij dat de herstart zonder enig overleg is uitgevoerd, zodat de veiligheidsregio niet in de gelegenheid was zich voor te bereiden om de mogelijke gevolgen. Het ROT had verwacht dat KPN dit vooraf zou overleggen, zodat afdoende maatregelen konden worden voorbereid.

Veiligheidsregio Zuid-Holland Zuid

In de veiligheidsregio Zuid-Holland Zuid zijn vanaf het begin van de KPN-storing C2000, P2000, de lijnen van het openbaar brandmeldsysteem en de binnenkomende lijnen voor de 112-meldingen zeer instabiel geweest. Soms was er verbinding, soms niet. De (gedeeltelijke) uitval was onvoorspelbaar. De brandweerposten in de veiligheidsregio zijn alle bemand om snel op brandmeldingen te kunnen reageren. Het was nog wel mogelijk om via mobiele telefoons op het Vodafone-netwerk verbinding te leggen met de kazernes. De veiligheidsregio heeft opgeschaald

[19] CIN staat voor Centraal Incidenten Nummer en wordt gebruikt in de Rotterdamse haven. Bij elke CIN-melding nemen vier instanties tegelijk de melding tot zich: politie, DCMR, brandweer en Havendienst. De CIN-melder, een bedrijf, wordt bevraagd volgens een vast vragenprotocol waarbij de politie het voortouw neemt en de andere instanties in principe alleen luisteren.

naar GRIP 2. Het kunnen voorzien in eigen communicatiemogelijkheden was een van de belangrijkste overwegingen hiervoor. Verder heeft de veiligheidsregio zoveel mogelijk ingespeeld op de ontwikkelingen. Met de vtsPN is contact gelegd over de tijdsduur van de storing en de verwachte hersteltijd.

De veiligheidsregio vraagt zich af in hoeverre voorbereiding op een dergelijke omvangrijke uitval mogelijk is. Een dergelijke uitval betreft een landelijk systeem, waarvoor een veiligheidsregio moeilijk of zeer slechts beperkt een back-upsysteem kan inrichten. Voor dit soort incidenten roept de veiligheidsregio de regionale crisisorganisatie bijeen die vervolgens, vanuit de daarin aanwezige professionaliteit, de verdere aanpak vorm geeft.

Veiligheidsregio Hollands Midden

In de veiligheidsregio Hollands Midden was sprake van uitval van C2000 in de Krimpenerwaard. Daarnaast was er een storingsindicatie voor ongeveer twee honderd directe lijnen van het openbaar brandmeldsysteem. De alarmering van eenheden via P2000 bleek, na een test, nog wel te werken. Ook was verbinding met eenheden mogelijk via gsm-telefoons. Bij alarmering van eenheden zou in het alarmbericht worden meegegeven dat de verbinding met de meldkamer via GSM-telefoons moest worden gemaakt. Met de instellingen waar de doormelding via het openbaar brandmeldsysteem niet mogelijk was is, voor zover daar personeel aanwezig was, contact gelegd om aan te geven hoe te handelen bij een brandmelding. De veiligheidsregio heeft overwogen op te schalen naar GRIP 2. Gezien het beperkte effect van de storing is daar van afgezien.

Veiligheidsregio Zeeland

In de veiligheidsregio Zeeland is een beperkt aantal vaste lijnen van de meldkamer naar onder andere ziekenhuizen uitgevallen. De veiligheidsregio heeft niet opgeschaald, omdat hiervoor volgens de veiligheidsregio geen directe aanleiding bestond. De technisch piketfunctionaris van de meldkamer heeft contact opgenomen met KPN met de vraag welke vaste lijnen waren uitgevallen. Met de betrokken instanties is vervolgens contact opgenomen, opdat zonodig via andere communicatiemiddelen contact gelegd kon worden.

De regio beschikt over een aantal satelliettelefoons, die bij uitval van de ‘normale’ verbindingen ook kunnen worden ingezet om de communicatie weer (deels) te herstellen. Ook beschikt de regio over een ‘video-conferencing-systeem’ waarmee contacten met de gemeentehuizen in Zeeland mogelijk is. Dit zou ook gebruikt kunnen worden als (een deel van) de communicatielijnen naar brandweerkazernes in de betreffende gemeenten uitvalt.

Vervoersbedrijf RET, Rotterdam

De RET beschikt over een mobilofoonnetwerk waarmee verbinding wordt onderhouden tussen de verkeersleiding en de metrobestuurders. Dit netwerk is eigendom van en wordt geëxploiteerd door KPN. De RET huurt het netwerk.
Het netwerk van de RET viel uit waardoor geen communicatie meer mogelijk was met de metrobestuurders. In tegenstelling tot tram- en busbestuurders die ‘normale’ verkeersdeelnemers zijn en eigenstandige beslissingen nemen, zijn metrobestuurders afhankelijk van het contact met de verkeersleiding. In de veiligheidsprocedures is bepaald dat het metronetwerk stilgelegd wordt als het communicatienetwerk niet beschikbaar is. Daar komt nog bij dat de beide rechtstreekse noodtelefoons met de alarmcentrale van de veiligheidsregio eveneens waren uitgevallen en ook beide aansluitingen van het Nationaal Noodnet bij de verkeersleiding bleken buiten werking te zijn. Bij eventuele calamiteiten kon dus ook geen contact opgenomen worden met de alarmcentrale van de veiligheidsregio. Dit was voor de RET een extra reden om het metroverkeer niet op te starten.

Het metronet kent een separate spoorbeveiliging, die ook zonder communicatie vanuit de verkeersleiding functioneert. De spoorbeveiliging is aangesloten op een eigen RET-netwerk en functioneert geheel autonoom. Hierdoor is de KPN-storing niet van invloed geweest op de spoorbeveiliging. De beschreven uitval van communicatievoorzieningen was voldoende reden om het metroverkeer niet op te starten.

Het contact tussen de verkeersleiding en de meldkamer van de veiligheidsregio Rotterdam-Rijnmond bleek via de aanwezige rechtstreekse lijnen, maar ook via het Nationaal Noodnet, niet mogelijk. Daardoor was de inzet van hulpdiensten bij eventuele incidenten beperkt geborgd en vond de RET het onverantwoord om de metro's te laten rijden.

De RET heeft de eigen crisisorganisatie in werking gesteld onder eenhoofdige leiding. Aan de verkeersleiding is een crisismanager toegevoegd en een crisismanager heeft als 'liaison' van de RET gefunctioneerd in het ROT van de veiligheidsregio.
Het metroverkeer is niet opgestart bij de aanvang van de dienstregeling, maar pas omstreeks half negen in de ochtend (na afloop van de storing) weer langzaam in bedrijf gesteld. De RET heeft overwogen vervangend vervoer in te zetten in de ochtendspits, maar hier uiteindelijk van afgezien. Het bleek niet haalbaar om voor het totale uitgevallen metroverkeer vervangend vervoer te regelen. De RET heeft via gerichte communicatie over de uitval van het metronetwerk met het publiek gecommuniceerd om de effecten beheersbaar te houden.

Luchtverkeersleiding Nederland (LVNL)

De lokale telecommunicatie-infrastructuur van de LVNL op de luchthaven Rotterdam - The Hague Airport die betrekking heeft op de verkeersleiding van het vliegverkeer is niet verstoord geweest. Wel is een groot aantal lijnen van de LVNL (ongeveer 130) uitgevallen. De directe effecten hiervan zijn zeer beperkt gebleven en waren slechts merkbaar in de systemen van Monitoring & Control op Schiphol die betrekking hadden op de luchthaven Rotterdam - The Hague Airport.

De LVNL beschikt over een crisisregeling met een escalatiemechanisme. Naarmate de verstoring ernstiger is, wordt de afhandelingscapaciteit van de betreffende luchthaven daarop aangepast. Bij aanvang viel de KPN-storing in de categorie 'reguliere verstoringen' (code LICHTGROEN) en zou de afhandelingscapaciteit van de luchthaven Rotterdam - The Hague Airport niet aangepast behoeven te worden. Wel zijn geconsigneerde personen opgeroepen om de storing te managen. Deze hebben contacten gelegd met KPN om de verwachte duur van de storing te vernemen. Ook hebben zij diverse systemen gereset.
Omdat onduidelijk was wanneer alle verbindingen weer hersteld zouden zijn, is rond 07:00 uur besloten over te gaan naar tot code GEEL ('verstoring met mogelijk effect op de capaciteit'). Kort daarop bleken alle verbindingen weer hersteld en is weer afgeschaald.

De LVNL gaat binnenkort gebruik maken van het Mustang-netwerk waarbinnen verbindingen naar het netwerk dubbel uitgevoerd worden. De verbindingen kunnen dan via verschillende routes hun weg vinden.

Luchthaven Rotterdam-The Hague Airport

De luchthaven heeft in zeer beperkte mate hinder ondervonden van de uitval van het KPN-netwerk. Daarbij is de veiligheid van het vliegverkeer niet in het geding geweest. Wel is hinder ondervonden in het automatische bagage-afhandelingsysteem. Het afhandelen van de bagage moest hierdoor handmatig plaats vinden. Het is overigens niet met zekerheid aan te geven of de KPN-storing de uitval van het geautomatiseerde systeem heeft veroorzaakt. Er was geen noodzaak tot het nemen van speciale maatregelen.
Havenbedrijf Rotterdam

Voor het Havenbedrijf Rotterdam is de uitval zeer beperkt gebleven. De vitale communicatiestructuur van het Havenbedrijf verloopt via een eigen glasvezelnetwerk in de haven. Hierop zijn de verkeerscentrales en de radarposten aangesloten die essentieel zijn voor de veiligheid van het scheepvaartverkeer. Communicatie met schepen en de aan boord zijnde loodsen verloopt via de marifoon (VHF-radionetwerk). Dit netwerk is onafhankelijk van het KPN-netwerk. Alleen het waarschuwen van een loods dat deze zich naar een te beloodsen schip moet begeven, kan enige hinder hebben ondervonden. Het waarschuwen gebeurt via mobiele telefoon. Als een loods niet kan worden bereikt kan dit hoogstens leiden tot het aan de kade of buitengaats blijven liggen van een schip, omdat geen loods aan boord was. Het havenbedrijf heeft zelf geen maatregelen genomen om de veiligheid van het scheepvaartverkeer te garanderen, want er was geen sprake van een verstoring. Wel heeft een liaison van het havenbedrijf plaatsgenomen in het ROT van de veiligheidsregio.

In de media was sprake dat als gevolg van de KPN-storing een schip, geladen met LNG (vloeibaar gemaakt aardgas) 'door het oog van de naald' zou zijn gekropen. In werkelijkheid bleek dit schip aangemeerd te liggen aan de LNG-terminal op de Maasvlakte en stond men op het punt het LNG te gaan lossen. De communicatie hierover tussen schip en terminal gebeurt via mobiele telefoon. De liaison van het havenbedrijf in het ROT heeft zijn collega aan boord van dat schip meegedeeld dat de communicatie via mobiele telefoon op het punt stond uit te vallen. Daarop is het lossen van het schip uit voorzorg uitgesteld. De burgemeester van Rotterdam haalde dit in de persconferentie op 28 juli 2011 aan als goed voorbeeld van proactief optreden in de Rotterdamse haven. Hoewel de veiligheid niet in gevaar is gekomen, is wel economische schade ontstaan.

Waterleidingbedrijven en waterschappen

De waterleidingbedrijven Evides en Oasen hebben geen uitval van cruciale lijnen ondervonden. Wel zijn enkele communicatievoorzieningen uitgevallen. De primaire processen in de drinkwatervoorziening konden echter blijven functioneren zonder deze communicatievoorzieningen. De waterleidingbedrijven hebben geen specifieke maatregelen hoeven nemen.

Het waterschap Hollandse Delta heeft geen hinder ondervonden van de storing. De uitgevallen lijnen betroffen waarschijnlijk 'normale' telefonieverbindingen. Het waterschap heeft geen specifieke maatregelen hoeven nemen. De communicatieverbindingen van het Waterschap maken gebruik van IP-netwerken (internet-gerelateerd) en zijn daarom niet afhankelijk van het vaste netwerk van KPN.

Voor het Hoogheemraadschap van Schieland en de Krimpenerwaard is de uitval zeer beperkt gebleven en heeft deze niet geleid tot effecten op de primaire processen. Het meet- en regelsysteem van het hoogheemraadschap kan ook bij uitval van deze lijnen blijven functioneren. Het hoogheemraadschap heeft geen specifieke maatregelen hoeven nemen. In tegenstelling tot het waterschap Hollandse Delta maken de communicatieverbindingen bij het hoogheemraadschap gebruik van 'vaste' DSL-lijnen.

3.3.3 Analyse

De betrokken veiligheidsregio's

Uit het onderzoek blijkt dat in de vier betrokken veiligheidsregio's cruciale verbindingen zijn uitgevallen. In drie veiligheidsregio's (Rotterdam-Rijnmond, Zuid-Holland Zuid en Hollands Midden) vielen de C2000-verbindingen uit en in twee regio's (Rotterdam-Rijnmond en Zuid-Holland) ook het

alarmeringssysteem P2000. Ook vielen het Nationaal Noodnet en verbindingen van het openbaar brandmeldsysteem uit.

De Veiligheidsregio's Rotterdam-Rijnmond en Zuid-Holland Zuid hebben de meeste last ondervonden van de storing. Beide regio's hebben ook opgeschaald naar GRIP 2 en de regio Rotterdam-Rijnmond op enig moment zelfs naar GRIP 4. Rotterdam-Rijnmond koos hiervoor omdat – op het moment dat het maatschappelijk leven ontwaakte – de storing nog niet was verholpen. De regio voorzag in elk geval een aanzienlijke verkeerscongestie.
Voor de veiligheidsregio Hollands Midden was opschaling niet noodzakelijk gezien het beperkte effect van de storing in die regio. Hetzelfde gold voor de veiligheidsregio Zeeland

Uit het onderzoek komt naar voren dat de veiligheidsregio's voortvarend reageerden op de storing en direct maatregelen troffen om de negatieve effecten van de storing, zowel op het functioneren van de eigen organisatie als het maatschappelijk leven, te minimaliseren. Doordat de uitval plaatsvond is deze aan velen onopgemerkt voorbij gegaan. Dit maakte dat de negatieve gevolgen beperkt waren.

De veiligheidsregio's hebben tevoren geen informatie over de werkzaamheden ontvangen. Ook was er geen communicatie over de 'koude herstart'. De veiligheidsregio's hadden dit wel van KPN verwacht om eventueel maatregelen te kunnen voorbereiden. De veiligheidsregio's hebben over het ontbreken van de benodigde informatie hun verwondering uitgesproken, omdat zij nadrukkelijk anders hadden verwacht.

Voor wat betreft de uitval van C2000 merken de inspecties het volgende op. C2000 is een landelijk systeem waarvan de veiligheidsregio's eindafnemers zijn. Veiligheidsregio's hebben slechts zeer beperkt invloed bij het optreden van storingen in het systeem en/of de afhandeling daarvan. Ook het monitoren van de storingen om, daarop anticiperend, maatregelen te kunnen treffen voor de operationele taakuitvoering, blijkt bijzonder lastig. De organisaties die binnen de netwerkstructuur van C2000 directer met KPN te maken hebben (zoals IVENT en de vtsPN) ondervinden bij een storing niet de druk van optredende problemen in de publieke veiligheid, zoals de veiligheidsregio's dat nadrukkelijk wel ervaren. Dit roept de vraag op of IVENT en de vtsPN zich als *directe* afnemers van de telecomdiensten van KPN bij storingen niet nadrukkelijker zouden moeten manifesteren.

De andere vitale organisaties

De RET heeft het meest direct te maken gehad met de negatieve effecten van de uitval van de cross connect. Het bedrijf zag zich genoodzaakt het metroverkeer niet op te starten. Doordat de storing in de nachtelijke uren plaatsvond bleef de overlast beperkt, maar dit werd anders toen de ochtendspits op gang kwam en de storing nog niet was opgelost. In de regio Rotterdam maken dagelijks ongeveer 600.000 personen gebruik van het openbaar vervoer en de uitval van een zo belangrijke verbinding als het metronet heeft flinke consequenties, niet alleen voor de RET maar ook voor de mensen en de organisaties die afhankelijk zijn van het vervoer.

De andere in het onderzoek betrokken vitale organisaties hebben beperkt of geen hinder ondervonden en ook nauwelijks maatregelen hoeven nemen. Ook hierbij geldt dat het feit dat de storing in de nachtelijke uren plaatsvond en hierdoor aan velen voorbij ging.

3.4 VOORBEREIDING VITALE ORGANISATIES OP UITVAL

Van veiligheidsregio's en andere vitale organisaties mag worden verwacht dat zij zijn voorbereid op mogelijke uitval van essentiële voorzieningen en dit ook in een continuïteitsplan opnemen. Het onderzoek richt zich daarom mede op de vraag in hoeverre de vitale organisaties daadwerkelijk invulling geven aan het continuïteitsmanagement.

Aan de bij het onderzoek betrokken organisaties is gevraagd of een uitval als deze is opgenomen in de risicoanalyse en of de organisaties over een calamiteiten- of continuïteitsplan beschikken, waarin voorbereide maatregelen zijn opgenomen om de effecten van mogelijke uitval te minimaliseren. Tevens is de vraag voorgelegd of de toepassing van de genomen maatregelen aanleiding heeft gegeven om continuïteitsplannen op te stellen of bestaande continuïteitsplannen te wijzigen.

3.4.1 Bevindingen

Deze paragraaf bevat een overzicht van de bevindingen per onderzochte organisatie. Eerst komen de vier betrokken veiligheidsregio's aan de orde. Vervolgens wordt aandacht besteed aan de voorbereiding door de andere betrokken vitale organisaties.

Veiligheidsregio Rotterdam-Rijnmond

De veiligheidsregio Rotterdam-Rijnmond besteedt in de risicoanalyse beperkt aandacht aan een incident zoals zich in juli 2011 heeft voorgedaan. Het enkelvoudig uitvallen van een deel van het communicatienetwerk is voorzien, maar een meervoudige storing niet. De veiligheidsregio is bezig met het opstellen van een continuïteitsplan. De KPN-storing in de Waalhaven en andere recente stroomstoringen in Rotterdam hebben ervoor gezorgd dat de veiligheidsregio hogere prioriteit toekent aan het opstellen van het continuïteitsplan. Het 'gestapeld' uitvallen van communicatievoorzieningen wordt hierin meegenomen.

Veiligheidsregio Zuid-Holland Zuid

De veiligheidsregio Zuid-Holland Zuid heeft enkelvoudige uitval van communicatievoorzieningen opgenomen in de risicoanalyse, meervoudige of algehele uitval niet. De veiligheidsregio werkt aan een continuïteitsplan, waarvoor verschillende bouwstenen inmiddels gereed zijn. De KPN-storing is voor de veiligheidsregio op dit moment geen aanleiding om de in gang gezette activiteiten voor het continuïteitsplan bij te stellen.

Veiligheidsregio Hollands Midden

De veiligheidsregio Hollands Midden heeft een omvangrijke uitval van communicatievoorzieningen zoals het incident in de Waalhaven te Rotterdam niet opgenomen in het risicoprofiel. De KPN-storing is wel aanleiding om hier nog eens nadrukkelijk naar te kijken. De veiligheidsregio is bezig met het opstellen van een continuïteitsplan. Delen hiervan zijn inmiddels afgerond. De KPN-storing is voor de veiligheidsregio op dit moment geen aanleiding tot bijstelling.
De regio beschikt over een convenant met de Dutch Amateur Radio Emergency Service (DARES). Deze zendamateurs kunnen in crisissituaties, waarbij communicatievoorzieningen zijn uitgevallen, een deel van de communicatie weer tot stand brengen middels radioverbindingen.

Veiligheidsregio Zeeland

De veiligheidsregio Zeeland heeft enkelvoudige uitval van communicatievoorzieningen opgenomen in de risicoanalyse, meervoudige of algehele uitval niet. De veiligheidsregio beschikt niet over een continuïteitsplan en heeft ook geen plannen om hiertoe te komen. Andere ontwikkelingen krijgen een hogere prioriteit. De veiligheidsregio is wel voornemens om – als wordt besloten tot het opstellen van een continuïteitsplan - een dergelijke uitval van communicatievoorzieningen hierin wel mee te nemen.
De veiligheidsregio Zeeland heeft wel, evenals de veiligheidsregio Hollands Midden, een convenant afgesloten met DARES.

Vervoersbedrijf RET, Rotterdam

Het vervoersbedrijf RET heeft in het calamiteitenplan rekening gehouden met de uitval van een deel van het communicatienetwerk. De RET beschikt over 'bedrijfscalamiteitenprocedures' om de werking van het openbaar vervoer in Rotterdam tijdens een storing zo goed mogelijk te laten verlopen. Hierbij is ook aandacht voor de juiste (voorbereide) maatregelen die getroffen moeten worden bij verstoringen. De KPN-storing is voor de RET op dit moment geen aanleiding om de plannen bij te stellen.

Luchtverkeersleiding Nederland (LVNL)

De Luchtverkeersleiding Nederland heeft de uitval van deze specifieke KPN-verbindingen niet voorzien in de risicoanalyse, omdat deze verbindingen maar voor een beperkt deel van invloed zijn op de primaire processen. De LVNL heeft de uitval van (een deel van) de technische infrastructuur wel opgenomen in de crisisregeling. De LVNL beschikt over een Regeling Crisisbeheersing die is gericht op de primaire processen van de organisatie. Aan veiligheid worden ten behoeve van de luchtverkeersdienstverlening geen concessies gedaan. Zo nodig wordt de intensiteit van het vliegverkeer teruggebracht. Het aantal vluchten wordt dan beperkt tot het niveau waarop het vanuit het oogpunt van veiligheid verantwoord is. De KPN-storing is voor de LVNL op dit moment geen aanleiding om de plannen bij te stellen.

Luchthaven Rotterdam-The Hague Airport

De primaire processen van de luchthaven Rotterdam-The Hague Airport richten zich op veilig en ongestoord vliegverkeer. Deze processen zijn deels belegd bij de LVNL (zowel het vliegverkeer in de lucht als de vliegtuigen taxiënd op het vliegveld) en deels bij de luchthaven zelf. De KPN-storing is voor de luchthaven op dit moment geen aanleiding om de plannen bij te stellen.

Havenbedrijf Rotterdam

Het havenbedrijf Rotterdam beschikt over een eigen glasvezelnetwerk en is hierdoor voor de tele- en datacommunicatie niet afhankelijk van KPN. De uitval op 27 juli 2011 had dan ook geen effect op de bedrijfsprocessen van het havenbedrijf. Om die reden is dit scenario ook niet opgenomen in de risicoanalyse. Het havenbedrijf beschikt over een continuïteitsplan. De KPN-storing is voor het Havenbedrijf Rotterdam op dit moment geen aanleiding om de plannen bij te stellen.

Waterleidingbedrijven en waterschappen

De waterleidingbedrijven Evides en Hollandse Delta beschikken over een plan om de vitale processen in de levering van drinkwater zo ongestoord mogelijk te laten verlopen.

Het waterschap Hollandse Delta heeft een continuïteitsplan voor de primaire processen. Het Hoogheemraadschap van Schieland en de Krimpenerwaard heeft de primaire processen voorzien van een back-up, voor het geval een van de 'normale' verbindingsmogelijkheden uitvalt. In het uiterste geval kan op handbediening worden overgegaan. Het continuïteitsplan kent vier stadia van verstoring van de primaire processen. Hiervoor zijn maatregelen benoemd gericht op het continueren van deze processen.

De KPN-storing is voor de waterleidingbedrijven en waterschappen op dit moment geen aanleiding om de plannen bij te stellen.

3.4.2 Analyse

De betrokken veiligheidsregio''s

Uit het onderzoek blijkt dat de veiligheidsregio's zich bewust zijn van het belang van continuïteitsmanagement voor de veiligheid in hun verzorgingsgebied. Drie van de vier betrokken veiligheidsregio's (Rotterdam-Rijnmond, Zuid-Holland Zuid en Hollands Midden) zijn ook daadwerkelijk bezig met het opstellen van een continuïteitsplan. Zij geven hiermee uitvoering aan de al sinds enkele jaren uitgezette lijn om serieus aandacht te besteden aan de continuïteit van de dienstverlening, ook onder kritische omstandigheden. En hoewel de plannen nog verdere verbetering behoeven zijn in deze al wel belangrijke stappen gezet.

Uit het onderzoek komt tevens naar voren dat de veiligheidsregio Zeeland ervoor heeft gekozen andere prioriteiten voorrang te geven en vooralsnog niet over te gaan tot het opstellen van en continuïteitsplan. Dit is een opmerkelijke keuze. Hoewel er vandaag de dag veel op de veiligheidsregio's afkomt en de beschikbare capaciteit moet worden verdeeld over diverse werkzaamheden, mag dit geen reden zijn continuïteitsmanagement een lage prioriteit te geven. De continuïteit van de dienstverlening in relatie tot het niveau van veiligheid in het verzorgingsgebied maakt de noodzaak tot het hebben van een continuïteitsplan evident. De burger mag dit zonder meer van de overheid verwachten. Niet voor niets gaat de handleiding continuïteitsmanagement van de overheid hier uitvoerig op in. In dit opzicht is de keuze van de veiligheidsregio Zeeland dan ook niet verstandig en is het raadzaam een andere koers in te zetten. Zeeland is een regio met veel risico's en de uitval van vitale voorzieningen kan leiden tot ongewenste maatschappelijk effecten.

De andere vitale organisaties

De andere vitale organisaties kennen meer nog dan de veiligheidsregio's een hoge prioriteit toe aan continuïteitsmanagement. Naast bedrijfseconomische overwegingen speelt hierbij de maatschappelijke verantwoordelijkheid nadrukkelijk mee. Uit het onderzoek komt naar voren dat met name de vitale organisaties in de transportsector veiligheid hoog in het vaandel hebben. Continuïteit van de bedrijfsvoering is hieraan in principe ondergeschikt. De plannen voorzien er in dat - als de veiligheid niet kan worden gegarandeerd - het vlieg-, rail- en scheepvaartverkeer wordt stopgezet. Dit is ook tijdens de storing in de Waalhaven gebleken. De RET heeft het metroverkeer niet opgestart tot de storing was verholpen en het lossen van een vrachtschip, dat op het moment van de storing lag aangemeerd aan de LNG-terminal op de Maasvlakte, is uit voorzorg uitgesteld. De overige vitale organisaties hebben geen verdere actie hoeven te ondernemen, omdat de gevolgen van de storing voor hen beperkt waren.

De vitale organisaties houden in hun continuïteitsplannen rekening met gedeeltelijke uitval van voorzieningen. Totale uitval is in de meeste plannen niet opgenomen. Gelet op de ervaringen bij het incident in de Waalhaven zou verwacht mogen worden dat de vitale organisaties de

continuïteitsplannen op dit punt nog eens kritisch zouden bezien. Uit het onderzoek komt echter naar voren dat zij dit niet in de planning hebben opgenomen. Voor een deel wordt dit ingegeven door het besef maar voor een (beperkt) deel afhankelijk te zijn van KPN. Havenbedrijf Rotterdam beschikt bijvoorbeeld over een eigen glasvezelnetwerk en is hiermee niet afhankelijk is van KPN. Daarnaast speelt mee dat de daadwerkelijke overlast van het incident voor vrijwel alle vitale organisaties gering was.

4 CONCLUSIES

Op basis van het onderzoek komen Agentschap Telecom en de Inspectie VenJ tot de volgende conclusies.

4.1 Risicobeheersing bij KPN

- **Onduidelijkheden rond Service Level Agreements**
  KPN baseert haar risicomanagement op het kunnen nakomen van de afspraken die in SLA's zijn vastgelegd. Hier zijn twee aandachtspunten bij te benoemen.
  1. Het is echter voor afnemers niet altijd duidelijk wat de SLA-afspraken exact inhouden. De rekenmethode die KPN hanteert om de beschikbaarheid te bepalen is bijvoorbeeld niet helder vastgelegd. De basis onder KPN's risicobeoordelingen is daarom onduidelijk.
  2. Door deze onduidelijkheid kan bij klanten het idee leven dat zij een hoger serviceniveau krijgen dan KPN daadwerkelijk levert. De verwachtingen die KPN, bewust of onbewust, bij haar klanten wekt, komen niet overeen met de werkelijkheid. Hierdoor kunnen klanten hun eigen risicomanagement baseren op verkeerde aannames en onbedoeld meer risico lopen.

- **Beperkte waarde van Life Cycle Management**
  Het Life Cycle Management voldoet aan de eisen die KPN daar zelf aan gesteld heeft. Vanwege de dubbele uitvoering van onderdelen in de DXC, zou het afdoende moeten zijn om voldoende reserveonderdelen op voorraad te houden. KPN wist echter in 2002 al dat de dubbele uitvoering van componenten niet in alle gevallen voldoet. Er zijn meerdere incidenten met DXC's geweest die toch tot uitval van de dienst hebben geleid. Uit het onderzoek is niet gebleken dat de eerder voorgestelde verbetermaatregelen daadwerkelijk zijn uitgevoerd. KPN wist dat de aannames bij het LCM proces niet altijd geldig zijn en dat het LCM proces bepaalde technische risico's ongedekt liet. Er zijn geen extra maatregelen getroffen om deze risico's op andere wijze te dekken.

- **Informatievoorziening tijdens incidenten**
  De categorie-indeling van klanten waarover de afdeling Zakelijke Markt beschikt, is niet automatisch beschikbaar voor TPM. De relatie tussen klant, de aard van het gebruik en de technische realisatie moet handmatig worden gelegd.
  Zonder de relatie tussen verbindingen en klanten vervalt ook de mogelijkheid om risicospreiding te verzorgen door vitale lijnen te verdelen over verschillende DXC's of deze te koppelen aan de nieuwste DXC's, met kortere opstarttijd. De meest urgente verbindingen kunnen hierdoor ook niet met voorrang worden hersteld. Dit beïnvloedt de impact van het incident negatief.
  In geval van storingen kan dan ook niet direct rekening worden gehouden met de prioriteit van de klant. KPN benoemt dit zelf als verbeterpunt.

4.2 Oorzaak en aanpak van de storing

KPN onderscheidt zich positief op een aantal aspecten.

- **Goede voorbereiding**
  Gesteld kan worden dat het geplande onderhoud van 26 op 27 juli 2011 voldoende is voorbereid. Er is een draaiboek gebruikt waarin de onderhoudsprocedure voor de voedingsconvertor is beschreven. Er is geen aanleiding om te veronderstellen dat Alcatel-Lucent (die het onderhoud heeft uitgevoerd in opdracht van KPN) deze procedure niet heeft

gevolgd. De onderhoudswerkzaamheden op zichzelf hebben daarmee geen onaanvaardbaar extra risico met zich meegebracht.
Ook was de beschikbaarheid van reserve onderdelen tijdens de verstoring van 26 op 27 juli 2011 toereikend.

- **Adequate aanpak storing**
  Nadat de verstoring was opgetreden heeft het escalatieproces van KPN, Be Alert, goed gefunctioneerd. Het incident is binnen een aanvaardbare tijd opgelost. De samenwerking tussen KPN en Alcatel-Lucent is goed en tijdens de verstoring was tweede en derdelijns expertise van Alcatel-Lucent goed beschikbaar en van hoog niveau.

- **Succesvolle migratie**
  De migratie van de verbindingen van de getroffen DXC naar een andere DXC is onder grote tijdsdruk uitgevoerd en goed verlopen. KPN heeft de migratie met ondersteuning van Alcatel-Lucent uitgevoerd. Het feit dat een vervangende DXC direct beschikbaar was heeft bijgedragen aan het verminderen van het potentiële risico op vervolguitval.

Een aantal zaken is voor verbetering vatbaar.

- **Verontreiniging**
  In de RCA zijn metaalresten in de DXC aangetroffen, wat een onwenselijk en vermijdbaar risico is, zeker omdat KPN wel een schoon werk-protocol hanteert.
  De RCA suggereert dat tot twee maal toe een metaaldeeltje precies zo in de DXC is gevallen dat een spanningsdip ontstond. Hieruit mag echter niet worden geconcludeerd dat verontreiniging ten grondslag ligt aan de verstoring van de DXC.

- **Geen noodscenario voor langdurige en/of totale uitval DXC**
  De veronderstelde onafhankelijkheid van componenten ten opzichte van elkaar in de DXC blijkt niet juist te zijn. Door volledig te vertrouwen op de dubbele uitvoering van componenten heeft KPN risico gelopen.
  Er is bij het geplande onderhoud geen rekening gehouden met de mogelijkheid dat de DXC ook na de 'koude herstart' niet zou functioneren en dus volledig zou uitvallen. Er is daarmee geen rekening gehouden met een noodscenario.
  De aanname dat zodra een component in de DXC kapot gaat de dubbele uitvoering ervan KPN de tijd geeft om dit te repareren gaat niet meer automatisch op.

Kans op herhaling

Binnen Nederland zijn nog 88 DXC's van hetzelfde type binnen de KPN-infrastructuur. Ook op deze locaties kan –zonder tegenmaatregelen- met een vergelijkbare kans een vergelijkbare verstoring optreden. De impact van een vergelijkbare verstoring kan vooral in stedelijk gebied vergelijkbaar zijn met de impact van de verstoring op 26 en 27 juli 2011, afhankelijk van de locatie en de bezettingsgraad van de betreffende DXC.

4.3 Maatschappelijke effecten van de uitval

- **Hinder en overlast**
  Vrijwel alle in het onderzoek betrokken vitale organisaties hebben in meerdere of mindere mate hinder of overlast ondervonden van de KPN-storing in de Waalhaven te Rotterdam. De primaire processen van de hulpverleningsdiensten en de overige onderzochte organisaties hebben niet te maken gehad met effecten die de gezondheid of veiligheid van personen direct aangetast hebben. Dat de maatschappelijke effecten van de storing gering waren was voor een belangrijk deel te danken aan het feit dat de storing in de nachtelijk uren plaatsvond. Uitval tijdens de dag- en avonduren had voor veel ernstiger hinder en overlast gezorgd.

- **Uitval van cruciale systemen**
  De storing trad op tijdens onderhoudswerkzaamheden en trof systemen die cruciaal zijn voor de hulpverleningsdiensten. In drie veiligheidsregio's viel het communicatiesysteem C2000 gedeeltelijk uit en in twee veiligheidsregio's voor een deel ook het alarmeringssysteem P2000. Ook het Nationaal Noodnet en verbindingen van het openbaar brandmeldsysteem vielen uit. Dat KPN de veiligheidsregio's tevoren niet op de hoogte stelde van het onderhoud hebben de regio's als een omissie ervaren.

- **Voortvarende aanpak**
  De veiligheidsregio's en de andere vitale organisaties hebben voortvarend gereageerd op de storing. In een aantal veiligheidsregio's is de crisisorganisatie gealarmeerd om adequaat te kunnen inspelen op de gevolgen van de uitval. De operationele hulpdiensten hebben maatregelen getroffen om bij incidenten de hulpverlening zo goed mogelijk doorgang te laten vinden.

- **Geen concessies aan veiligheid**
  Binnen de onderzochte organisaties in de transportsector (de metro en het vlieg- en scheepvaartverkeer) worden geen concessies gedaan aan de veiligheid van het vervoer. Als de omstandigheden maken dat het transport niet veilig kan plaatsvinden, gebeurt dit niet of beperkt. Zo kan het metroverkeer worden stilgezet, het vliegverkeer worden afgebouwd of omgeleid en blijven schepen aan de kade of buitengaats. Op die manier is de veiligheid voor zowel passagiers als omgeving gewaarborgd. Hiermee geven de vitale organisaties op adequate wijze invulling aan hun maatschappelijke verantwoordelijkheid.

4.4 Voorbereiding vitale organisaties op uitval

- **Continuïteitsmanagement**
  Alle onderzochte bedrijven en organisaties in de vitale sectoren beschikken over (delen van) een continuïteitsplan of een vergelijkbaar plan om de primaire 'vitale' processen zo ongestoord mogelijk doorgang te kunnen laten vinden. Bij de veiligheidsregio's zijn deze plannen nog volop in ontwikkeling, waarbij zij gebruik maken van de 'Handleiding continuïteitsmanagement voor organisaties met een vitale maatschappelijk functie', die het ministerie van Veiligheid en Justitie eind 2010 beschikbaar stelde. De andere vitale organisaties beschikken over meer uitgebreide continuïteitsplannen, die vooral zijn toegespitst op de primaire processen.

- **Bewustwording mogelijkheid grootschalige uitval**
  Veiligheidsregio's beseffen maar ten dele dat de uitval van communicatievoorzieningen zodanig grootschalig kan zijn, dat operationele hulpdiensten en andere vitale en/of maatschappelijke organisaties hun taken niet meer naar behoren kunnen uitvoeren.
  Organisaties als de RET, de Luchtverkeersleiding Nederland en het Havenbedrijf Rotterdam zijn zich meer dan de veiligheidsregio's bewust van de gevolgen van uitval van

communicatievoorzieningen en hebben de gedeeltelijke uitval van voorzieningen ook in continuïteitsplannen opgenomen.
Een continuïteitsplan dat rekening houdt met een totale uitval van communicatievoorzieningen, zoals bij het incident in de Waalhaven het geval was, is echter nergens aangetroffen. Voor een aantal organisaties is dit ook niet noodzakelijk, omdat zij de risico's hebben gespreid en niet alleen van KPN afhankelijk zijn.

- **Praktische alternatieven**
  Een aantal veiligheidsregio's beschikt over alternatieven, die in geval van uitval de communicatieverbindingen voor de operationele diensten beperkt kunnen overnemen. Een veiligheidsregio beschikt over satelliettelefoons en twee veiligheidsregio's hebben een convenant afgesloten met een organisatie voor zendamateurs. Hiermee kan de communicatie voor een deel worden overgenomen bij algehele uitval.

5 AANBEVELINGEN

Op basis van het onderzoek doen Agentschap Telecom en de Inspectie VenJ de volgende aanbevelingen.

Aan KPN

- Leg de rekenmethoden achter de SLA-afspraken helder vast en deel deze met afnemers.
- Verkrijg inzicht in de toepassingen waarvoor klanten hun verbinding inzetten, zodat de prioriteiten van klanten beter inzichtelijk worden.
- Verbeter de koppeling tussen klantgegevens en verbindingsgegevens, zodat de impact van verstoringen sneller bepaald kan worden en bij het herstel rekening kan worden gehouden met de prioriteiten van klanten.
- Houd rekening met volledige en langdurige uitval van systemen en werk noodscenario's hiervoor uit.
- Neem alle passende, technische en organisatorische maatregelen om uitval in de andere 88 DXC's te voorkomen, waaronder - indien nodig - het preventief vervangen van (onderdelen van) klokkaarten.
- Informeer de veiligheidsregio's en andere vitale organisaties vooraf over onderhoudswerkzaamheden waarbij risico's bestaan voor het uitvallen van cruciale systemen.

Aan de besturen van de veiligheidsregio's en de andere vitale organisaties

- Wees u bewust van de kwetsbare positie van uw organisatie waar het gaat om de telecommunicatievoorzieningen. Ondanks een hoog SLA is (totale) uitval een reëel risico.
- Stel vast welke mate van uitval van het telecommunicatienetwerk acceptabel is, ervan uitgaande dat 100% zekerheid niet bestaat. Inventariseer welke alternatieve vormen van telecommunicatie geschikt zijn om bij (gedeeltelijke) uitval in de communicatiebehoefte te voorzien.
- Zorg voor een continuïteitsplan waarin, mede op basis van het risicoprofiel, aan de hand van crisisscenario's staat beschreven op welke manier cruciale processen doorgang kunnen vinden.
- Beoefen het scenario waarbij sprake is van (gedeeltelijke) uitval van communicatievoorzieningen
- Maak voor een optimale doorgang van de communicatie (ook tijdens crisisomstandigheden) afdoende afspraken met de aanbieders van telecommunicatievoorzieningen.
- Maak afspraken met KPN over het tevoren geïnformeerd worden over onderhoudswerkzaamheden, waarbij risico's bestaan voor het uitvallen van cruciale systemen.
- Verleen inzicht in de toepassingen waarvoor verbindingen worden ingezet, zodat gezamenlijk met KPN een rangorde van verbindingen bepaald kan worden.
- Stel u op de hoogte van de rekenmethoden van SLA-afspraken en kies voor cruciale verbindingen een SLA van voldoende hoog niveau.

Aan de minister van Defensie en de minister van Veiligheid en Justitie

Draag er zorg voor dat IVENT en de vtsPN zich in geval van een storing nadrukkelijk als klant namens de veiligheidsregio's naar KPN toe manifesteren.

BIJLAGE

LIJST MET AFKORTINGEN EN BEGRIPPEN

ALU	Alcatel-Lucent
AT	Agentschap Telecom
ATM	Asynchronous Transfer Mode
AU	Administrative Unit (module in de DXC)
Be Alert	Escalatie- en crisismanagement procedure (KPN)
BSD	Business Service Desk (KPN)
C2000	Communicatiesysteem voor de hulpverlening
CM	Segment Consumentenmarkt (KPN)
Cross connect	Zie DXC
DAP	Document Afspraken en Procedures
DARES	Dutch Amateur Radio Emergency Service
DTO	Defensie Telematica Organisatie (Zie IVENT)
DXC	Digital Cross Connect
E1	Vaste verbinding van 2 Mbit/s
EMC	Electromagnetic Compatibility
ETN	Ethernet Transport Netwerk
GMK-ZHZ	Gemeenschappelijke Meldkamer Zuid-Holland Zuid
GRIP	Gecoördineerde Regionale Incidentbestrijdings Procedure
GSM	Global System for Mobile Communications
ICT	Informatie en Communicatie Technologie
Inspectie VenJ	Inspectie Veiligheid en Justitie
IP	Internet Protocol
ITNL	IT organisatie (KPN)
IVENT	Bedrijfsgroep 'Informatievoorziening en – Technologie' van het ministerie van Defensie
Klokkaart	Master Clock Board (zie MCB)
KPI	Key Performance Indicator
KPN	Koninklijke PTT Nederland
LCM	Life Cycle Management
LNG	Liquefied Natural Gas
LVNL	Luchtverkeersleiding Nederland
Master Klokkaart	Zie MCB
MCB	Master Clock Board (kaart in de DXC)
MCTN	Managed Customer Transmission Network
MMT	Matrix Maintenance Tool (Alcatel-Lucent)
N&S	Networks 7 Services (KPN)
Netcool	Monitoring systeem voor netwerkelementen
NIPA	Netwerk, IP & Access (-diensten) (KPN)
NOC	Network Operations Center (KPN)
OAM	Operationeel Account Manager (KPN)
OLA	Operational Level Agreement
P2000	Netwerk voor alarmering van hulpverleningsdiensten
PoP	Point of Presence
PSTN	Public Switched Telephone Network

RCA	Root Cause Analyse
Regiekamer	Afdeling voor geplande werkzaamheden (KPN)
RET	Rotterdamse Electrische Tramweg
ROT	Regionaal Operationeel Team
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SPoF	Single Point of Failure
STM-1	Vaste verbinding van 155 Mbit/s
TEC	Technical Excellence Center (Alcatel-Lucent)
UMS	Unit Meldkamer Systemen
Voedingsconverter	Module in de DXC
VPN	Virtual Private Network
VRR	Veiligheidsregio Rotterdam-Rijnmond
vtsPN	voorziening tot samenwerking Politie Nederland
W&O	Wholesale en Operations (KPN)
ZM	Segment Zakelijke Markt (KPN)