# Bijlage 7

kpn

Datum
20 september 2018

Uw brief van
21 juni 2018

Ons Kenmerk
2018-U-00034-RvB

Contactpersoon

Telefoon

E-mail

Bijlagen
x

Agentschap Telecom

Piet Mondriaanlaan 54
3812 GV AMERSFOORT

**Reactie Inspectierapport zorgplicht continuïteit en bereikbaarheid 112**

Geachte

Graag reageer ik op de conclusies en aanbevelingen van het Inspectierapport van 21 juni met kenmerk AT-EZK/7636572 van dit jaar.

We herkennen de conclusies, en ook de aanbevelingen zijn voor ons relevante aandachtspunten.

Ik ga hieronder in op de kritische punten in de conclusies, en op de aanbevelingen.

**Conclusies.**
Op onderdeel B2 Assetmanagement hebben we op twee conclusies een terugkoppeling:

1. **Het statement dat is gemaakt:** *Voor consumenten wordt niet gewezen op de beschikbaarheid en de eventuele impact.*
   **Reactie KPN:**
   KPN onderschrijft het belang van het informeren van consumenten over de beschikbaarheid van de aangeboden diensten. Dit doet zij op dit moment onder meer in de algemene voorwaarden (zie daarvoor bijvoorbeeld het hoofdstuk van de algemene voorwaarden voor het mobiele abonnement en hoofdstuk 5 van de algemene voorwaarden voor internet) en via de website https://www.kpn.com/service/storingen.htm#/problemen-en-storingen. We bezien of we hierover nog transparanter kunnen zijn zodat eindgebruikers zich nog beter bewust kunnen zijn van mogelijke onderbrekingen in de continuïteit en duur en omvang daarvan.

2. **Het statement dat is gemaakt:** *Er is geen monitoring op de mobiele en vaste 112 diensten.*
   **Reactie KPN:**
   KPN voert monitoring uit op al haar diensten. Onderdeel hiervan is monitoring op bellen naar 112 via de mobiele of vaste infrastructuur.

   De monitoring op 1-1-2 bellen is dus een integraal onderdeel van de monitoring van de reguliere voice diensten zelf, zowel bij mobiel als VoIP. Als een gebruiker kan bellen naar een willekeurig nummer geldt dat ook voor 1-1-2, en omgekeerd. Daarmee is de bewaking van 1-1-2 ook geborgd.

Raad van Bestuur
Wilhelminakade 123
3072 AP ROTTERDAM

Telefoon (070) 451 01 05

Correspondentieadres:
Postbus 25110
3001 HC ROTTERDAM

KPN BV
KvK nr. 27124701
NL009292056B01

Voor de verwerking in het 1-1-2 domein (dat betreft het contract met de Politie waarvoor we strenge kwaliteitseisen hebben afgesproken) is monitoring gewaarborgd met een speciaal ketenmonitoringssysteem dat alle aspecten binnen het KPN technische 1-1-2 domein (specifieke 1-1-2 infrastructuur) bewaakt. Elementen die worden gemonitord met dit systeem omvatten: connectiviteit naar de openbare infrastructuur, connectiviteit naar de 1-1-2 aannamecentra en alle regionale meldkamers, connectiviteit op verbindingen binnen het technische 1-1-2 domein (glasvezel), bewaking van het serverpark (incl. applicaties) en bewaking van de centralistenapplicatie. Deze monitoring vindt 24X7 plaats waarbij beheer en opvolging wordt uitgevoerd door het KPN Service Quality Center.
De vaste openbare infrastructuur wordt eveneens bewaakt tot aan het koppelpunt van de mobiele operators.
KPN heeft overigens alleen zicht op het functioneren van de technische keten van haar eigen mobiele netwerk, niet van de andere mobiele operators. Ook is er geen zicht op het functioneren van de infrastructuur in de regionale meldkamers.

**Aanbevelingen.**
Per aanbeveling geven we onze reactie.

B1: Beleid, Governance en risicomanagement

1. *Betrek ook de diensten niet zijnde vitaal en kritiek in voldoende mate bij het continuïteitsbeleid.* **Reactie KPN:** We hebben de BCM-proces stappen ((B)IA, RA/RTP en Continuïteitsplannen) bij de vitale en kritieke diensten de hoogste prioriteit gegeven. Voor de overige diensten willen we hetzelfde proces toepassen, zoals KSP voorschrijft. Dit wordt momenteel in het ol gerealiseerd en deels al ondersteund.

B2: Assetmanagement

2. *Verifieer het risicomanagement proces in hoeverre de jaarlijkse uitvoering het beoogde doel bereikt.*
   **Reactie KPN:** KSP vereist dat elk kwartaal de voortgang van het implementeren van vastgestelde maatregelen in het risicomanagement proces wordt gerapporteerd. gaat daarin helpen door elk kwartaal de verantwoordelijke voor de maatregelen te vragen de rapportage op te leveren. Achterblijvende vorderingen worden zo zichtbaar, waardoor extra management attentie kan worden gegeven.
3. *Verifieer in hoeverre de locatie van*

   **Reactie KPN:** De acties zijn reeds uitgezet om op locatie te controleren of de genomen maatregelen conform de KSP-eisen zijn. Eventuele tekortkomingen worden opgelost en risico's gemitigeerd.
4. *Informeer consumenten over de beschikbaarheid van de aangeboden diensten.*
   **Reactie KPN:** Zie hiervoor de reactie op de betreffende conclusie hierboven.

B4: Voorbereiding contingencies en herstel

5. *Draag er zorg voor dat KPN als vitale partner onderdeel gaat uitmaken van de huidige informatievoorziening tussen de huidige crisispartners (met name de netbeheerders in het bijzonder) gedurende calamiteiten en crisis.*
   **Reactie KPN:** Onderstaande ontwikkelingen gaan de informatiedeling tussen crisispartners verbeteren:
   - Het verkrijgen van directe nummers van (regionaal) Netbeheerders is via het NCO-T aangekaart bij ministerie van Economische Zaken en Klimaat. Het belang en de noodzaak om elkaar over en weer te kunnen bereiken wordt door het ministerie herkend en hier wordt aan gewerkt in de vorm van een website waar over energieonderbrekingen wordt gerapporteerd samen met de herstelprognoses, toegankelijk voor vitale sectoren, waaronder de Telecomsector.
   - Daarnaast loopt ook via het NCO-T het traject Netcentrisch Werken, waarbij beoogd wordt op het informatiemanagement van de Veiligheidsregio's aan te sluiten. Dit traject omvat de nodige stappen, opleidingen en mogelijk ook opzet van tooling waardoor over en weer het informatiebeeld van crises en calamiteiten kan worden aangevuld. Dit traject vergt wel de nodige doorlooptijd, en zal niet voor 2019 gereed zijn.

Ik hoop hiermee te hebben laten zien dat we als KPN de conclusies en aanbevelingen ter harte nemen en daar opvolging aan geven.

Mochten er over bovenstaande nog vragen zijn dan horen wij die uiteraard graag.

Met vriendelijke groet,

CEO en Voorzitter Raad van Bestuur

# Bijlage 8

**Date**
December 2017

**Version**
2.0



# KPN Continuïteitsplan ten behoeve van de Telecomwet

***KPN***

Confidential

**Date**
December 2017

**Version**
2.0



# Contents



***Document geschiedenis***

| *Versie* | *Datum* | *Auteur* | *Commentaar* |
|---|---|---|---|
| v1.0 | Maart 2013 | | Initiële versie verzonden aan AT |
| v1.1 | November 2013 | | Aanpassing tbv audit AT (update van links in appendix A) |
| V2.0 | December 2017 | | Update voor KSP 2.0;<br>Toevoegen Continuïteitsaspecten hoge Opstelpunten; |

# 1 Inleiding

In de TelecomWet en het Besluit Continuïteit wordt van aanbieders van openbare telecommunicatie netwerken en openbare telecommunicatie diensten geëist dat zij een continuïteitsplan hebben. Het Agentschap Telecom, dat namens de overheid toeziet op de uitvoering van dit deel van de wet en het besluit, heeft richtlijnen opgesteld waaraan dit continuïteitsplan moet voldoen [20]. Hieruit blijkt dat het Agentschap een andere, bredere, definitie gebruikt voor het begrip continuïteit dan KPN.
Het Agentschap beschouwt alle elementen die de beschikbaarheid van diensten kunnen beïnvloeden als relevant voor een continuïteitsplan, beginnend bij beheer in een normale situatie en eindigend bij langdurige en ernstige onbeschikbaarheid van diensten, dus van availability-, change-, incident-, calamiteiten-, continuity management en uitlopend in crisismanagement.
KPN gebruikt voor de term continuïteit de scope zoals die is gedefinieerd in de BS25999 / ISO22301 standaard voor Business Continuity. Hierin is een continuïteitsplan beperkt tot de set aan maatregelen die de kans op optreden en de gevolgen van een calamiteit moeten minimaliseren.

Om in dit document verwarring te voorkomen tussen een continuïteitsplan in de zin van de TW of zoals die bij KPN wordt gehanteerd zal de volgende conventie worden gebruikt:

**TW Continuïteitsplan:** continuïteitsplan zoals dit in de TW geëist wordt (dit document);
**KPN Continuity plan:** continuïteitsplan zoals dat intern KPN gehanteerd wordt (ook **KPN SCP**, **KPN BCP** of **KPN TRP** zie de afkortingenlijst voor de betekenis hiervan)

Dit document beschrijft het continuïteitsplan in de definitie van het Agentschap zoals dat bij KPN is ingericht. Omdat alle processen die onder deze scope vallen reeds zijn ingericht bij KPN, wordt in dit document geen nieuwe inhoud gecreëerd maar wordt volstaan met een korte omschrijving en een verwijzing naar andere documentatie. De structuur van het document volgt om dezelfde reden de structuur van het document waarin het Agentschap de minimale eisen voor een continuïteitsplan definieert [20]. Deze eisen van het Agentschap zijn in kaders weergegeven.

## 2 Continuïteitseisen algemeen

**I Continuïteitseisen algemeen**

- Aanbieders beschrijven in het continuïteitsplan welke 'passende' technische en organisatorische maatregelen zij hebben genomen om de risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen.
- Aanbieders van openbare telefoondiensten en aanbieders van openbare elektronische communicatie netwerken waarover openbare telefoondiensten worden aangeboden beschrijven in het continuïteitsplan welke 'noodzakelijke' maatregelen zij kunnen nemen om, in geval van een technische storing of uitval van het elektriciteitsnetwerk, de beschikbaarheid van hun telefoondienst te garanderen.

### 2.1 Assurance / Technisch beheer

Diensten die KPN aan de Nederlandse markt levert, worden beheerd vanuit het Service Quality Center (SQC) in Alle dagelijkse beheer vindt hier plaats. Vanuit het SQC worden alle relevante beheerprocessen bestuurd, van de operationele monitoring van de KPN netwerken tot aan het allerlaatste escalatiemoment bij grote regionale of landelijke calamiteiten.
Onderdeel van het SQC is het Security Operating Center (SOC), waar de KPN infrastructuur wordt gemonitord op het optreden van beveiligingsincidenten.

### 2.2 Incident Management

Zodra incidenten optreden treedt het BeAlert proces [16] in werking. In dit proces wordt nauwkeurig beschreven welke maatregelen en welke besturing worden gehanteerd bij een bepaalde impact van de verstoring. Elk 'niveau' dat hierin onderkend wordt heeft een kleurcode, variërend van groen (klein incident, geringe impact, lokaal, binnen SLA, meerdere incidenten per dag) via blauw en geel naar oranje (grote impact, regionaal of landelijk, imagoschade, treedt incidenteel op). De kleurcodes, bijbehorende impact en ook het bijbehorende besturingsmechanisme zijn intern KPN zeer bekend. Voor security incidenten is een enigszins afwijkende BeAlert procedure opgesteld [13] vanwege de potentieel gevoelige informatie, maar het proces volgt gelijke stappen en escalatie methoden als het 'normale' BeAlert proces.

Optredende incidenten worden op het KPN intranet gepubliceerd [24], en voor een belangrijk deel ook op het Internet [25].

### 2.3 KPN Continuity Management

Een onderdeel van het incident/calamiteiten management proces is de mogelijkheid om, als dit nodig wordt geacht, een KPN Business Continuity Plan in werking te stellen om de dienstverlening vanuit een andere locatie of vanaf andere systemen te herstellen. KPN Business Continuity Management is een integraal onderdeel van KPN Security Policy (KSP), waar zowel op proces niveau [4] als op governance niveau [3] eisen worden gesteld aan de KPN organisatie en het formaat en de inhoud van KPN Continuïteitsplannen die mogelijk moeten worden opgesteld en geoefend [6, 7, 8]. Momenteel loopt een

programma om alle KPN Business Continuity plannen op te nemen in een repository . dat ook benaderbaar is in geval van grote incidenten.

Eind 2017 heeft de Raad van Bestuur het besluit genomen om voo N diensten zeer scherpe eisen te stellen voor de continuïteit [19]: maximale verstoringsduur treedt maximaa jaar op, impact is maximaal eindgebruikers door uitval van een eigen infrastructuur element en hooguit regionaal van aard. De diensten die hieronder vallen zijn gekozen omdat ze voor KPN essentieel zijn voor het uitvoeren van haar strategie en het voortbestaan van KPN, maar ook vanuit maatschappelijk perspectief. Gekoppeld aan de kritieke diensten is ook aangegeven welke panden van KPN van groot belang zijn voor het behalen van de hier boven beschreven doelstellingen [19]. Voor de kritieke diensten worden de benodigde maatregelen om de afgesproken beschikbaarheid waar te maken via het KSP BCM proces. Voor de zijn ook afspraken gemaakt met de veiligheidsregio's over bewaking en surveillance.

Nota Bene: zowel de lijst met kritieke diensten, als de lijst met kritieke panden wordt jaarlijks heroverwogen.

### 2.4 Crisis Management

Op het moment dat impact of duur van een verstoring zo groot worden dat een oplossing niet meer binnen het normale BeAlert incident- en calamiteiten management kan worden beheerst, dan kan het ultieme escalatie proces 'Code Rood' [21] worden ingeroepen.
Dit gebeurt alleen in werking bij zeer grote verstoringen met landelijke impact waarbij het voortbestaan van KPN op het spel staat.
Het an ook worden afgeroepen naar aanleiding van potentiële grote verstoringen van een andere aard, zoals Human Resources (o.a. pandemie, staking) of grote landelijke calamiteiten (o.a. overstroming). Voor een aantal scenario's zijn informatiesets opgesteld aan de hand eerdere ervaringen of ervaringen bij andere partijen..

### 2.5 Innovatie / Functioneel beheer

Om de continuïteit van dienstverlening ook te waarborgen bij wijziging van infrastructuur, diensten of platformen, stelt KSP eisen aan Innovatie: 'Beveiligingsmaatregelen bij innovatie en ontwikkeling'. Als onderdeel daarvan wordt gedurende het innovatietraject de checklist Requirements Innovations gebruikt om te voorkomen dat projectplannen security en/of continuïteitsrisico's introduceren. Toetsing vindt decentraal plaats, maar de toetsmomenten en toetsmethode tooling gestandaardiseerd [1].

**I Continuïteitseisen algemeen**

- Aanbieders beschrijven in het continuïteitsplan hoe men het systeem van voortdurende verbetering van de continuïteit beheert en beheerst en licht dit toe. Binnen deze systematiek worden alle 'passende en noodzakelijke' technische en organisatorische maatregelen als bedoeld in de continuïteitswetgeving in het plan geadresseerd, uitgevoerd, gecontroleerd en geëvalueerd.

KSP schrijft implementatie van een BCM proces [4] gebaseerd op de plan-do-check-act cyclus voor. In de cyclus is de continu verbetering van KPN Business Continuity het leitmotif [4].

Nota Bene: KPN is voortdurend bezig om haar security en business continuity beleid aan te scherpen. De hier gemelde processen en documenten zijn de status zoals die gold eind 2017, maar kunnen op het moment van een mogelijke audit door het Agentschap vervangen zijn door nieuwe versie(s).

## 3 Hoge Opstelpunten

Op 1 januari 2018 zijn extra eisen gesteld aan de continuïteit van Hoge Opstelpunten. De Telecomwet stelt dat hiervoor een 'gezamenlijk continuïteitsplan' dient te worden gemaakt.

> **Besluit Continuïteit 5b:**
> **1d.** Een beschrijving van de wijze waarop wordt gerealiseerd dat het gezamenlijke continuïteitsplan en de daarin beschreven afstemming van maatregelen bij veranderende omstandigheden worden aangepast.

KPN heeft hiervoor met de marktpartijen een Convenant afgesloten. Dit Convenant omvat voorschriften rondom het ontwerp, de bouw en het beheer van Hoge Opstelpunten. In lijn met hoofdstuk 2 van dit document. Daarnaast zijn de risico's rondom 'Hoge Opstelpunten' beschreven, maatregelen benoemd met daarbij de verantwoordelijke partij (inclusief de functionaris) [29] [30].

## 4 Continuïteitseisen t.a.v. personeel

**II Continuïteitseisen t.a.v. personeel**

- De aanbieder dient te vermelden welke kundige functionaris binnen de organisatie verantwoordelijk is voor het beheren en beheersen van het systeem, waarbij gestreefd wordt naar voortdurende verbetering van de continuïteit.

De KPN Chief Information Security Officer is verantwoordelijk voor definitie en onderhoud van het KPN Business Continuity beleid en toezicht op naleving. Uitvoering van het beleid vindt decentraal plaats in de bedrijfsonderdelen.

**II Continuïteitseisen t.a.v. personeel**

- De aanbieder noteert in het continuïteitsplan de contactgegevens van deze functionaris(en).

## 5 Fysieke beveiliging en beveiliging van de omgeving

**III Fysieke beveiliging en beveiliging van de omgeving**

- De aanbieder legt bevoegde personen, betrokken bij, de voor de veiligheid en integriteit van het netwerk relevante processen, een geheimhoudingsverplichting op. Aanbieders lichten dit proces inclusief de selectiecriteria toe in het continuïteitsplan.

KPN heeft in KSP een sectie opgenomen betreffende Beveiligingseisen personeel [9].
Bij in dienst treden moeten werknemers de voor hen van toepassing zijnde 'deelcodes' doornemen, gevolgd door een toets. Dit proces wordt jaarlijks doorlopen. In de Deelcode 3 - 'Zo gaan we om met informatie, communicatie & bedrijfsmiddelen' wordt expliciet aandacht gegeven aan classificatie van gegevens, en hoe daar mee moet worden omgegaan [26].
Voor indiensttreding moeten werknemers een VOG verklaring overleggen, voor gevoelige functies wordt een nader onderzoek ingesteld (screening). Bovendien moet de werknemen een geheimhoudingsverklaring [27] tekenen.
Een vertrouwelijksheids clausule is een standaard onderdeel van alle contracten met leveranciers en outsourcing partners conform KSP 'Beveiligingsmaatregelen voor leveranciers' [10].

**III Fysieke beveiliging en beveiliging van de omgeving**

- De aanbieder licht in het continuïteitsplan toe op welke manier hij zorg draagt voor een deugdelijke beveiliging van zijn netwerk of dienst waardoor er slechts toegang wordt verschaft aan daartoe gemachtigde personen. Met name waar het:

  1. de fysieke toegang tot gebouwen of faciliteiten betreft en
  2. de logische toegang tot informatie en informatie verwerkende systemen betreft die van belang zijn voor de veiligheid of integriteit van netwerk of dienst.

KPN heeft beleid voor fysieke beveiliging van al haar panden [15, 11, 12]. Daarnaast wordt alleen toegang verleend op basis van een toegangspas (Company Card) [28]. Dit beleid wordt actief bewaakt .

KPN heeft beleid voor de logische toegang tot applicaties en componenten [14], structurele invulling hiervan gebeurt via de Identity en Access Management portal [14a]. Autorisaties worden bepaald aan de hand van het functieprofiel van een medewerker. Uitgegeven autorisaties worden minimaal 1 maal per jaar geverifieerd door de leidinggevende. Remote toegang tot het KPN kantoren netwerk gebeurt doormiddel van een VPN constructie, waarbij de toegang wordt verstrekt na two-factor authenticatie.

Toegang wordt verleend op basis van Toegang op afstand beleid [2].

**III Fysieke beveiliging en beveiliging van de omgeving**

- De aanbieder dient in het continuïteitsplan te beschrijven dat slechts de daartoe bevoegde personen op de hoogte zijn van de inhoud van het continuïteitsplan en/of toegang hebben tot het continuïteitsplan.

Alle beleidsdocumenten op het vlak van continuïteit zijn gemarkeerd als "KPN intern", waardoor deze alleen intern KPN gedistribueerd mogen worden. Ingevulde templates, waaronder KPN continuity plannen, hebben de classificatie "vertrouwelijk", waardoor zij alleen voor direct betrokkenen bestemd zijn [9].

## 6 Melden van een inbreuk op de veiligheid of een verlies van integriteit

**IV Melden van een inbreuk op de veiligheid of een verlies van integriteit**

- De aanbieder dient in het continuïteitsplan te beschrijven welke functionaris, in geval van een inbreuk op de veiligheid of een verlies van integriteit, verantwoordelijk is voor het doen van een melding. Deze, in Nederland gevestigde, functionaris treedt tevens op als eerste aanspreekpunt van de aanbieder voor het meldpunt.

Melding van verstoringen aan het AT is beschreven in het KPN incidentmanagement proces 'BeAlert'. Dit proces wordt gecoördineerd door aangewezen functionarissen in het Service Quality Center (SQC). Deze dienstenmanagers hebben qualitate qua toegang tot de meldingen site van het Agentschap. [16, 22]. In het proces is beschreven welke informatie bij de melding moet worden gegeven.
Omgekeerd kan het SQC benaderd worden door het AT mocht de noodzaak daartoe bestaan.
Het SQC en de post dienstenmanager is 7*24 bezet

**IV Melden van een inbreuk op de veiligheid of een verlies van integriteit**

- De aanbieder dient het proces van melding van een incident in het continuïteitsplan te beschrijven. Vooralsnog betekent dit dat de melding in ieder geval: het tijdstip van aanvang van het incident; de aard en de omvang van het incident; op welk netwerk en/of bij welke dienst het incident heeft plaatsgevonden en een prognose van de hersteltijd moet bevatten.

De procedure voor het aan- en afmelden van een incident is beschreven in [22].

## 7 Risicobeheer voor de veiligheid en de integriteit

**V Risicobeheer voor de veiligheid en de integriteit**

- De aanbieder inventariseert, beoordeelt en evalueert regelmatig de risico's voor de veiligheid en de integriteit van zijn netwerken en diensten. Hij verwerkt de resultaten hiervan in het continuïteitsplan.

Onderdeel van het KSP BCM Beleid [4], is dat 1 maal per jaar Business impact en risico's voor de diensten die KPN aan de markt levert worden bepaald [4, 17, 18]. Dit gebeurt zowel voor security als voor continuïteitsaspecten. De uitkomst van het BIA/RA proces kan resulteren in het creëren van een Risico Behandelplan, waarin acties kunnen worden opgenomen die voor continuïteit kunnen variëren van het aanpassen van de infrastructuur, tot het maken en/of aanpassen van KPN Business Continuity plannen.

**V Risicobeheer voor de veiligheid en de integriteit**

- Majeure incidenten worden in een apart hoofdstuk binnen het continuïteitsplan beschreven. Deze beschrijving bevat in ieder geval: het tijdstip van aanvang van het incident; de aard en de omvang van het incident; op welk netwerk en bij welke dienst het incident heeft plaatsgevonden en de hersteltijd van het onderhavige incident. De beschrijving van het incident wordt aangevuld met het pakket aan maatregelen dat de aanbieder heeft genomen om het risico op herhaling te minimaliseren.

Een integraal onderdeel van het BeAlert proces [16] is dat incidenten worden geëvalueerd, dit wordt aangestuurd door de SQC Bij evaluatie van ernstige incidenten is de diensteigenaar betrokken, die gebaseerd op de uitkomst kan besluiten om (delen van) de infrastructuur te laten aanpassen, of om KPN Business Continuity plannen aan te passen. Alle evaluaties worden bij het SQC opgeslagen.

Voor het / Code Rood [21] geldt een vergelijkbare werkwijze, alleen ligt de verantwoordelijkheid voor de evaluatie bij CISO, waar ook proces verantwoordelijkheid is belegd.

## Afkortingen

| | |
|---|---|
| BCM | Business Continuity Management |
| BCP | KPN Business Continuity Plan |
| BIA | Business Impact Analyse |
| BS | British Standard |
| ISO | International Organisation for Standardisation |
| KSP | KPN Security Policy |
| MAD | Maximum Acceptable Data loss |
| MTPD | Maximum tolerable period of disruption |
| PDCA | Plan Do Check Act or Deming Cycle |
| RA | Risk Assessment |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SCP | KPN Service Continuity Plan |
| SLA | Service Level Agreement |
| SQC | Service Quality Center |
| TRP | KPN Technical Recovery Plan |
| VPN | Virtual Private Network |

# Appendix A Referenties (update t.o.v. versie 1.1)

[1]
[2]
[3]
[4]
[5]
[6]
[7]
[8]
[9]
[10]
[11]
[12]
[13]

[14]

[15]
[16]

[17]
[18]

[19]

[20]
[21]

[22]
[23]
[24]
[25]
[26]
[27]
[28]
[29]
[30]

# Bijlage 9

Agentschap Telecom
*Ministerie van Economische Zaken en Klimaat*

# Plan van aanpak onderzoek storing telefoniedienstverlening (inclusief 112) en NL-Alert bij KPN

## Colofon

| | |
|---|---|
| Aan | |
| Van | |
| Nummer | Definitief |
| Datum | 10 september 2019 |
| Leden | |

# Inhoud

# 1 Inleiding

## 1.1 Aanleiding

Agentschap Telecom stelt, bij het uitvoeren van haar missie "Agentschap Telecom waarborgt de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken, zodanig dat Nederland veilig verbonden is", het maatschappelijk belang centraal. Incidenten in de telecomsector kunnen economisch en maatschappelijk veel schade aanrichten. Een aantal processen[1] binnen de telecom/ICT-sector is eind 2017 aangemerkt als vitaal. Vitale processen zijn processen die bij uitval of verstoring tot ernstige maatschappelijke ontwrichting kunnen leiden. Met het oog op het maatschappelijk belang is het vanzelfsprekend dat de continuïteit van netwerken en/of diensten op een zo hoog mogelijk peil blijft of wordt gebracht en de maatschappelijke en economische impact van incidenten en calamiteiten tot het minimum wordt beperkt. Dit draagt bij aan het vertrouwen in de telecom/ICT-sector.

Op 24 juni 2019 vonden er twee storingen plaats bij KPN. Ten eerste vond er een storing plaats in het telefonienetwerk van KPN met landelijke gevolgen. De maatschappelijke impact van de storing was groot, vaste en mobiele telefonie voor klanten van KPN was uitgevallen. Tevens was het alarmnummer 112 in het hele land onbereikbaar geworden, niet alleen voor de KPN klanten maar ook voor de klanten van de andere twee mobiele telefonieaanbieders VodafoneZiggo en T-Mobile. Dit gold ook voor alle vaste KPN telefonie klanten.
Ook was het 0900 nummer van de Politie door de KPN storing niet beschikbaar.
Ten tweede was er een verstoring in de NL-Alert dienst. Tijdens de onbereikbaarheid van het alarmnummer 112 dienstverlening waren NL-Alert berichten verstuurd over wat burgers konden doen als zij met spoed een hulpdienst nodig hadden. Door de verstoring in de NL-berichtendienst bij KPN was een deel van deze berichten niet of later bij de klanten van het KPN netwerk aangekomen.

## 1.2 Doel van het onderzoek

Het doel van het onderzoek is om op basis van de bevindingen aanbevelingen te doen die helpen om, binnen de telecomsector, soortgelijke verstoringen in de toekomst te voorkomen.

Het onderzoek zal tevens inzicht geven in de aard, oorzaak en afhandeling van de storingen, met daaronder begrepen de opbouw van het netwerk en de gemaakte keuzes. Ook zal onderzocht worden in hoeverre is voldaan aan de wettelijke eisen met betrekking tot de continuïteit en welke maatregelen genomen zijn of worden genomen om herhaling te voorkomen. Onderwerpen van onderzoek vormen de verstoorde telefoniedienst van KPN, waaronder de dienst 112, en NL-Alert.

[1] Internet en dataverkeer; internettoegang en datadiensten; spraakdiensten en sms; plaats- en tijdsbepaling middels gps

## 1.3 Centrale vraag en onderzoeksvragen

De volgende centrale vraag staat centraal:

*Wat was de oorzaak van de verstoringen en welke maatregelen kunnen worden getroffen om dergelijke storingen in de toekomst te voorkomen?*

Hiervoor zijn de volgende onderzoeksvragen geformuleerd:

1. Wat is er feitelijk gebeurd, wat waren de (dieperliggende) oorzaken van deze storingen?
2. Welke acties heeft KPN ondernomen om deze storingen te verhelpen danwel om herhaling te voorkomen?
3. Welke continuïteitsmaatregelen had KPN genomen ter voorkoming van dergelijk storingen?
4. Welke maatregelen worden getroffen om dergelijke verstoringen in de toekomst te voorkomen?

## 1.4 Afbakening

Het onderzoek richt zich op de impact van de uitval van de telefoniedienstverlening (inclusief 112) en NL-Alert van KPN op 24 juni 2019.

Het onderzoek richt zich niet op de crisiscommunicatie en het inhoudelijk informeren van de maatschappij. Het onderzoek richt zich ook niet op het perspectief vanuit de gebruikers, i.c. de weerbaarheid.

Indien Agentschap Telecom in dit onderzoek tot de conclusie komt dat er bij KPN mogelijk sprake zou zijn van verwijtbaarheid ten aanzien van continuïteit, zal dit onderwerp uit het onderzoek gehaald worden en een apart handhavingstraject gaan volgen.

# 2 Onderzoeksaanpak

## 2.1 Operationalisatie

Voor de beantwoording van de hoofdvraag en onderzoeksvragen wordt de volgende aanpak gekozen:

Ten eerste is gekozen voor een "proces onderzoek". Hierin wordt feitelijk beschreven wat er vanaf het begin van het incident is gebeurd.

Ten tweede wordt onderzocht in hoeverre de vooraf getroffen maatregelen hebben gewerkt. Hierbij worden de ENISA[2] guidelines[3] als uitgangspunt genomen. Dit kader wordt standaard door Agentschap Telecom gebruikt voor een inspectie. Dit kader wordt vervolgens gelegd op de KPN Security Policy (KSP) van KPN. Het KSP wordt door KPN gebruikt als guidelines voor de invulling van haar netwerk en diensten. Agentschap Telecom zal dit KSP aanvullen indien er relevante onderwerpen ontbreken en elementen schrappen die niet relevant zijn voor dit onderzoek (scope).

Op basis van de bevindingen worden conclusies getrokken die mogelijk leiden tot leer- en verbeterpunten in de vorm van aanbevelingen.

## 2.2 Methoden en technieken van onderzoek

**Documentanalyse**
De documentenanalyse is gebaseerd op verschillende bronnen. Voorbeelden hiervan zijn de formele uitvraag aan KPN door het Ministerie van Justitie en Veiligheid[4] inclusief het antwoord van KPN, het overleg tussen KPN en Agentschap Telecom op 16 juli 2019 en de rapportages bij Ministerie van Justitie en Veiligheid over de verzonden NL-Alert berichten op 24 juni 2019.
Bij KPN worden alle relevante documenten opgevraagd. Aangezien een groot deel bedrijfsvertrouwelijk is (door KPN aangegeven), zal de documentenanalyse vooral op locatie bij KPN plaats gaan vinden.
Tevens wordt informatie gebruikt die verzameld is uit de media.
Tot slot kunnen eerdere onderzoeken zoals "112 onder de loep" als informatiebron dienen.

**Interviews**
Interviews vinden plaats met betrokken medewerkers binnen KPN of andere organisaties. Hierbij moet gedacht worden aan medewerkers op zowel strategisch, tactisch en operationeel niveau. Van de interviews worden beknopte verslagen op hoofdlijnen opgesteld en ter verificatie van feitelijke onjuistheden voorgelegd aan de geïnterviewden.

[2] ENISA: European Union Agency for Network and Information Security
[3] Technical guidelines on security measures December 2014
[4] Brief aan KPN van 26 juni 2019 inzake storing bereikbaarheid 112 en 0900-8844 en beantwoording door KPN op 10 juli 2019

## 2.3 Fasen van het onderzoek

Het onderzoek bestaat uit drie fasen:

Fase 1: de voorbereiding van het onderzoek
In deze fase wordt onder andere het plan van aanpak opgesteld, afgestemd met de andere inspecties en afspraken gemaakt met KPN.

Fase 2: de uitvoering van het onderzoek
In deze fase ligt de nadruk op de uitvoering van het onderzoek op locatie bij KPN door middel van documentenonderzoek en interviews.

Fase 3: het opstellen en aanbieden van de rapportage
In de laatste fase wordt het rapport opgesteld, ter verificatie voor feiten voorgelegd aan KPN en aangeboden aan de staatssecretaris van Economische Zaken en Klimaat.

# 3 Samenhang andere onderzoeken

**Onderzoek Inspectie Justitie en Veiligheid (IJenV)**
IJenV richt zich op de crisiscommunicatie rondom de uitval van het alarmnummer 112. Daarbij kijkt IJenV hoe het traject is verlopen om de burger te informeren over de alternatieven voor het alarmnummer 112 en of gewerkt is conform de afspraken en procedures. Het doel van het onderzoek van IJenV is om lessen te trekken voor de toekomst in relatie tot de crisiscommunicatie. IJenV richt zich in dit onderzoek in elk geval op de Nationale Politie de landelijke 112-alarmcentrale van de Landelijke Eenheid van de politie, het ministerie van Justitie en Veiligheid en de 25 veiligheidsregio's inclusief de regionale meldkamers.

**Onderzoek Inspectie Gezondheidszorg en Jeugd (IGJ)**
IGJ is geïnformeerd over de consequenties die de 112-storing bij KPN heeft gehad voor de zorginstellingen in de acute keten volgens de gebruikelijke routine van (calamiteiten)meldingen. Zij inventariseert hoe de meest voor de hand liggende zorgorganisaties zijn omgegaan met de uitval van het alarmnummer 112, of bestaande protocollen en draaiboeken zijn gebruikt en of die toereikend waren.

**Onderzoek Instituut Fysieke Veiligheid (IFV)**
Het onderzoek van het IFV richt zich met name op de wijze waarop bovenregionaal afstemming is georganiseerd en de rollen van de regio's, politie-eenheden en de Rijksoverheid in hun onderlinge samenhang; de relaties en samenwerking. Enerzijds wordt gekeken hoe de samenwerking verliep, en anderzijds wordt de vraag gesteld hoe bij dergelijke 'gebiedsontbonden' crises nu op een goede manier samengewerkt zou kunnen worden. Daarbij zal de insteek niet operationeel gericht zijn, maar vooral bestuurlijk. Gezien de insteek van het onderzoek zal primair met bestuurders en leidinggevenden (regionaal en nationaal) gesproken worden.

Agentschap Telecom heeft haar onderzoek afgestemd op het onderzoek van IJenV en IGJ om onder andere de toezichtslast te beperken. Het streven is de publicatie van de onderzoeken van de drie toezichthouders gelijktijdig te laten verlopen.

**Onderzoek meldkamers**
Dit onderzoek richt zich op de continuïteit van de regionale meldkamers en de landelijke 112-alarmcentrale. Het onderzoek gaat in op de continuïteit op het gebied van personeel, gebouw en techniek en het opvolgen van de aanbevelingen van een eerder onderzoek naar de meldkamers in 2015.

# 4 Organisatie, planning en communicatie

## 4.1 Organisatie

Het onderzoeksteam is gevormd binnen de afdeling Veiligheid (Informatieveiligheid). Het bestaat uit vier leden:

- [redacted]

Gezien het maatschappelijke belang van het onderzoek, wordt er binnen de verschillende fasen van het onderzoek een beroep gedaan op specifieke expertise van andere teams/afdelingen:

- Publieke Veiligheid:
- Eidas
- Wbni
- ATS:
- S-Veiligheid:

Periodiek (maandelijks) vindt er afstemming plaats tussen de contactpersonen van de IJenV, IGJ en Agentschap Telecom.

## 4.2 Planning

De doorlooptijd van het onderzoek is van juni 2019 tot en met maart 2020. De planning op hoofdlijnen in verschillende fasen is als volgt:

- Fase 1 Voorbereiding van het onderzoek: juli 2019 – medio september
- Fase 2 Uitvoering van het onderzoek: september – november
- Fase 3a Opstellen rapportage: november - medio januari 2020
- Fase 3b Aanbieden rapportage: medio januari - medio maart 2020.

## 4.3 Risico's

Er is veel politieke bestuurlijke aandacht voor de storingen op 24 juni 2019. Tevens is hierdoor al een voorschot genomen op eventuele te nemen maatregelen. Van belang is dat het onderzoek leidt tot een juiste duiding van wat er feitelijk is gebeurd en van de genomen (vooraf) danwel te nemen (achteraf) maatregelen. Deze bevindingen zijn richtinggevend voor de aanbevelingen die Agentschap Telecom zal formuleren.

De drie inspecties hebben afgesproken periodiek (maandelijks) met elkaar af te stemmen gedurende de onderzoeken. Van belang is dat de inspecties blijven streven naar een gezamenlijke publicatie van de resultaten van de drie onderzoeken aangezien gekozen is voor een individuele aanpak.

Alle door KPN vertrouwelijk meegedeelde informatie, zowel in schriftelijke vorm als door middel van persoonlijke communicatie gedurende het veldwerk, zal binnen de kaders van de geldende wet- en regelgeving als dusdanig behandeld worden. Gezien

de vele bedrijfsvertrouwelijke documenten is afgesproken dat deze documenten op locatie worden ingezien[5].

## 4.4 Communicatie

**Voorafgaand aan het onderzoek**
KPN is via de vaste contactpersoon geïnformeerd over het instellen van het onderzoek dat in afstemming met IJenV en IGJ wordt uitgevoerd. KPN heeft aangegeven dat volledige medewerking aan het onderzoek wordt verleend. Ook vindt er op periodieke momenten contact plaats tussen Agentschap Telecom en KPN voor de goede voorbereiding en uitvoering van het onderzoek.

De beleidsmedewerkers van Economische Zaken en Klimaat (DE) zijn hierover nader geïnformeerd.

De drie inspecties hebben op 26 juni 2019 een gezamenlijk persbericht uitgebracht.

**Na het opstellen van de rapportage**
Op basis van de verzamelde en gevalideerde informatie vormt Agentschap Telecom zich een beeld en een oordeel van het onderzoeksthema. De opgestelde concept rapportage wordt ter verificatie voor mogelijke feitelijke onjuistheden voor een periode van twee weken aan KPN voorgelegd. Na verwerking van de wederhoor (dit wordt vastgelegd in een tabel zodat transparant is wat er met de opmerkingen is gebeurd.) en na interne vaststelling van het rapport wordt het rapport aangeboden aan de staatssecretaris van Economische Zaken en Klimaat voor het formuleren van een beleidsreactie. Het rapport wordt zes weken na aanbieding aan de staatssecretaris van Economische Zaken en Klimaat gepubliceerd. Het rapport wordt 48 uur voor publicatie aan KPN onder embargo verstrekt zodat KPN zich kan voorbereiden[6].

Er zal een gezamenlijk persbericht door de drie inspecties worden uitgebracht. S&C van Agentschap Telecom is hiervoor aangesloten.

[5] Deze werkwijze wordt door Agentschap Telecom toegepast op verzoek van de ondertoezichtgestelde.
[6] Vaste afspraak met de drie grote telecomaanbieders.

# Bijlage 10

Agentschap Telecom
*Ministerie van Economische Zaken en Klimaat*

**TER INFORMATIE**

Staatssecretaris van Economische Zaken en Klimaat

Emmasingel 1
9726 AH Groningen
Postbus 450
9700 AL Groningen
T (050) 587 74 44
F (050) 587 74 00
www.agentschaptelecom.nl
info@agentschaptelecom.nl

# nota

Aanbieding rapport Continuïteit meldkamers Agentschap Telecom en Inspectie Justitie en Veiligheid

**Datum**
8 augustus 2019

**Ons kenmerk**
AT-EZK/7825364

**Uw kenmerk**

## Aanleiding

Agentschap Telecom (hierna het agentschap) en Inspectie Justitie en Veiligheid (hierna de Inspectie) hebben een onderzoek uitgevoerd naar de continuïteit van meldkamers. Dit onderzoek is een vervolg op het onderzoek Meldkamers uit 2015 dat eveneens gezamenlijk door het agentschap en de Inspectie is uitgevoerd. Meldkamers – als onderdeel van de 112-keten – zijn van cruciaal belang voor een adequate en efficiënte hulpverlening. Echter de regionale meldkamers zijn kwetsbaar als het gaat om het waarborgen van de continuïteit van hun dienstverlening naar de maatschappij.
Uit de landelijke storing bij KPN op 24 juni 2019[1] werd nog weer eens duidelijk hoe groot de impact van een verstoring in de 112-keten is. Het is van levensbelang dat de continuïteit van die dienstverlening, waaronder die van de meldkamers, in de 112-keten goed geborgd is.

Het agentschap en de Inspectie onderzochten welke acties de meldkamers naar aanleiding van het vorige onderzoek Meldkamers hebben genomen om de continuïteit van de 112-dienstverlening te borgen. Het onderzoek richtte zich op de fase vanaf het moment dat de burger contact heeft met de landelijke 112-centrale tot en met het contact van de regionale meldkamer met de hulpdienst(en). Hierbij bied ik u het onderzoeksrapport aan met het verzoek er kennis van te nemen. Hierbij merk ik op dat het onderwerp van het onderzoek, continuïteit van meldkamers, niet uw verantwoordelijkheden raken.

## Advies

U kunt de nota lezen en voor kennisgeving aannemen.

[1] De Minister van Justitie en Veiligheid heeft in de Kamerbrief van 25 juni 2019 aangegeven deze storing nader te gaan onderzoeken. Daarbij zal de focus juist vooral liggen op die fase in de 112-keten voorafgaand aan het moment dat de burger contact heeft met de landelijke 112-centrale.

Daarnaast wil ik u vragen of u gebruik wilt maken van de mogelijkheid een beleidsreactie te formuleren op bijgevoegd rapport. Voor u goed om te weten dat de IG van de Inspectie het rapport onlangs heeft aangeboden aan de Minister van Justitie en Veiligheid met de vraag het rapport, al dan niet vergezeld van een beleidsreactie, binnen zes weken aan te bieden aan de Tweede Kamer.

**Kernpunten**

Het agentschap en de Inspectie concluderen dat:

- de verantwoordelijken voor de taakuitvoering van de regionale meldkamers naar aanleiding van de aanbevelingen uit het eerdere onderzoek naar de meldkamers nauwelijks maatregelen hebben genomen om de continuïteit ten aanzien van personeel, locatie en techniek voldoende te borgen. Daardoor zijn de regionale meldkamers nog steeds zeer kwetsbaar;
- de landelijke 112-centrale daarentegen diverse maatregelen heeft genomen om de continuïteit te verbeteren;
- de regionale meldkamers nog steeds geen gebruik maken van een integrale risicosystematiek om continuïteitsrisico's voldoende te borgen.
- het de meldkamers nog steeds ontbreekt aan een duidelijke verdeling tussen taken, rollen en verantwoordelijkheden bij lokaal beheer. Tevens ontbreekt nog immer een adequate PDCA[2]-cyclus voor de werkprocessen van beheer;
- de nieuwe aanpak door de LMS[3] een positieve werking heeft op de ontwikkelingen in het meldkamerdomein;
- de nieuwe aanpak om te komen tot een vanuit alle disciplines gedragen robuuste meldkamerorganisatie ambitieus en complex is en veel afhankelijkheden bevat en daarom een risico vormt;
- het bij alle betrokken partijen ontbreekt aan de urgentie om de continuïteit van de meldkamers, als onmisbare schakel voor de hulpvraag van de burger, nu eerst prioriteit te geven;
- het ontbreken van een uniforme invulling van de inrichting van beheer - na samenvoeging van twintig lokale beheerafdelingen en het MDC[4] tot een landelijke beheerorganisatie - een risico vormt;
- de perikelen rondom de transitie naar de LMO[5] hebben ervoor gezorgd dat er geen of in beperkte mate maatregelen zijn genomen naar aanleiding van de aanbevelingen van het eerdere meldkameronderzoek.

Het agentschap en de Inspectie doen de volgende aanbevelingen:

1. Borg de continuïteit van de meldkamers:
   a. Zorg ervoor dat meldkamers niet in die mate een terughoudend investeringsbeleid voeren dat sprake is van een tekort aan gekwalificeerd personeel. Terughoudendheid bij het aannemen van centralisten mag geen consequenties hebben voor de realisatie van de gewenste bezetting, het opleiden, trainen en oefenen en het bijdragen aan de ontwikkeling van de LMS;

[2] Plan, Do, Check en Act
[3] Landelijke Meldkamer Samenwerking
[4] Meldkamer Diensten Centrum
[5] Landelijke Meldkamer Organisatie