Inspectorate
Ministry of Justice and Security

Inaccessibility of emergency services number 112 on 24 June 2019

Investigation of actions taken by KPN, the Dutch government, the emergency services and care organisations

Index

Summary, conclusions and recommendations

1.1 Background

On Monday 24 June 2019, between 15:34 and 18:52, the telephone network of KPN B.V. (hereinafter KPN) malfunctioned. As a result, KPN customers were almost entirely unable to make or receive calls, including calls to the emergency services control centre. KPN's internet services continued to function during this time, so it was possible to make calls via WhatsApp or other web-based services. However, citizens were unable to call the emergency services number 112 to request assistance from the fire brigade, police or ambulance service. Other 0800- and 0900- numbers, such as the national police hotline 0900-8844, were also rendered inaccessible by the malfunction.

The 112 emergency services has been inaccessible several times throughout the course of its history, although this was the first time that this kind of breakdown affected the whole country and all callers. On the same day, KPN was also having technical issues with the NL-Alert service via 4G, although this issue was not connected to the malfunction of the telephone network. The NL-Alert malfunction persisted for nearly 24 hours, from 12:00 on the day in question until 11:40 the next day. In order to inform citizens of the malfunction affecting 112 and 0900-8844, NL-Alert messages were sent at both the regional and national levels. However, not a single user received any of these NL-Alert messages via KPN's 4G network.

In response to the malfunctions, the government bodies, emergency services and care organisations scaled up their crisis response organisations and the police and security regions took action to boost the accessibility and responsiveness of police stations, fire stations, etc. The emergency services staff, care organisations and government bodies used a variety of communication channels to inform citizens about the malfunctions and alternative ways to contact the emergency services. For this purpose, the security regions and the Ministry of Justice and Security made use of regional and national NL-Alert messages (respectively), among other methods. However, the NL-Alert messages did not function normally: in addition to KPN customers failing to receive NL-Alert messages via 4G, other citizens received regional NL-Alert messages from a different security region to the one they were in. Furthermore, the high volume of NL-Alert messages sent by the security regions and the Ministry of Justice and Security resulted in congestion of the central NL-Alert system, causing a delay in sending national and regional NL-Alert messages to the mobile network operators. The effect of this was that many citizens received these regional and national NL-Alert messages late (in some cases, extremely late). Furthermore, many citizens received a variety of alternative emergency numbers via both regional and national messages. One of the numbers listed in a national NL-Alert message turned out to be the tip line of the newspaper De Telegraaf. In addition to these NL-Alert messages, the government bodies, emergency services and care organisations also used social media to inform citizens of the situation, although both the quantity and the inconsistency of this information was excessive. On this particular day, there was insufficient capacity to organise clear communication with citizens and the media described the situation as chaotic.

By 18:52, the malfunction had been resolved and the 112 emergency services was once again accessible to citizens. By 21:00, all of the organisations had scaled down their crisis response organisations and at 21:30, a final NL-Alert message was sent to report the resolution of the issue.

The inaccessibility of the 112 emergency services, the chaotic communication and the resulting gaps in emergency healthcare services had a substantial impact on society. The events prompted investigations by Radiocommunications Agency Netherlands (hereinafter AT), The Inspectorate of Justice and Security (hereinafter IJ&V) and the Health and Youth Care Inspectorate (hereinafter IGJ).

1.2 Objectives, main questions and scope

AT investigated the inaccessibility of the 112 emergency services and the malfunctions affecting KPN's telephone and NL-Alert services. The objective of the investigation was to use the information gained to make recommendations that will help the telecom sector prevent similar malfunctions in the future. AT's main question was as follows: 'What was the cause of the malfunctions and what measures can be taken to prevent such malfunctions from recurring?'

IJ&V investigated existing policy and the actions taken at the time of the malfunction by three groups of actors: the Ministry of Justice and Security, the police and the security regions. The objective of the investigation was to identify what action was taken by these groups to guarantee the accessibility of the emergency services both in the run-up to and during the malfunctions at KPN. IJ&V's main question was as follows: 'What action was taken to guarantee the accessibility of the emergency services and was it carried out as planned?'

In line with its duties as a supervisory body, the IGJ's investigation sought to gain insight into the possible problems affecting aid organisations such as the Regional Medical Assistance Organisation (GHORs), the regional ambulance services (RAVs) and the out-of-hours GP services (HAPs) and in what way these problems were dealt with. The IGJ received reports from a number of RAVs concerning the death of a citizen during the malfunction of KPN's telephone services. However, the RAVs also reported that their responses to the incidents were within the standard time limits and in compliance with protocols. As a result, these reports are not included in the scope of this investigation, although brief explanatory notes are given. IGJ's main question was as follows: How did emergency aid organisations such as the GHORs, the RAVs and the HAPs respond to the inaccessibility of the 112 emergency services and the malfunction at KPN?

1.3 Findings and analysis

1.3.1 Situation prior to incident: policy, agreements and preparation

112 and voice services

When citizens require emergency assistance, they can call the emergency services via the emergency number 112. 112 traffic from all voice service providers - both mobile phones and land lines - is sent via KPN's telephone network to the public safety answer point 112 in Driebergen. An employee of the public safety answer point 112 then answers the 112 call and transfers the conversation to the regional emergency response centres of the required emergency service(s) in the security region corresponding to the caller's location at the time. The regional emergency response centre then alerts the required emergency service(s). The head of the police service serves as controller and therefore bears responsibility for the 112 domain. The Minister of J&S is responsible for the 112 chain (figure 1).

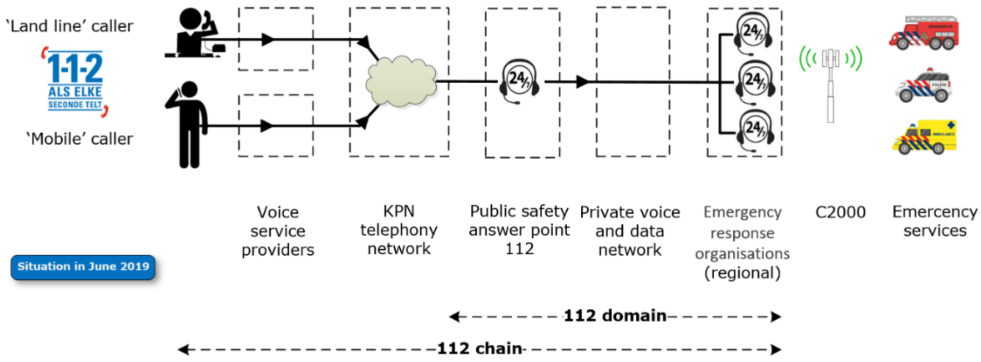

Figure 1. *The 112 chain (source: AT).*

NL-Alert

NL-Alert is a public warning system used by the government to rapidly provide messages to citizens containing information about emergency situations (figure 2). Primary responsibility for the use of NL-Alert is borne by the security regions. The creation and sending of NL-Alert messages is generally carried out via the security regions' regional emergency response centres.

Three types of account are authorised to create and send NL-Alert messages: regional, supraregional and national. The majority of the security regions or regional emergency response centres have a supraregional account that authorises them to send NL-Alert messages within their own security regions, as well as to neighbouring regions. The National Crisis Centre and the Central Netherlands Police

Unit both have a national account. NL-Alert messages are sent via the broker to the mobile network providers such as KPN, T-Mobile/Tele2 and VodafoneZiggo[1]. They send NL-Alert messages to mobile phones via their mobile networks using *Cell Broadcast technology*.

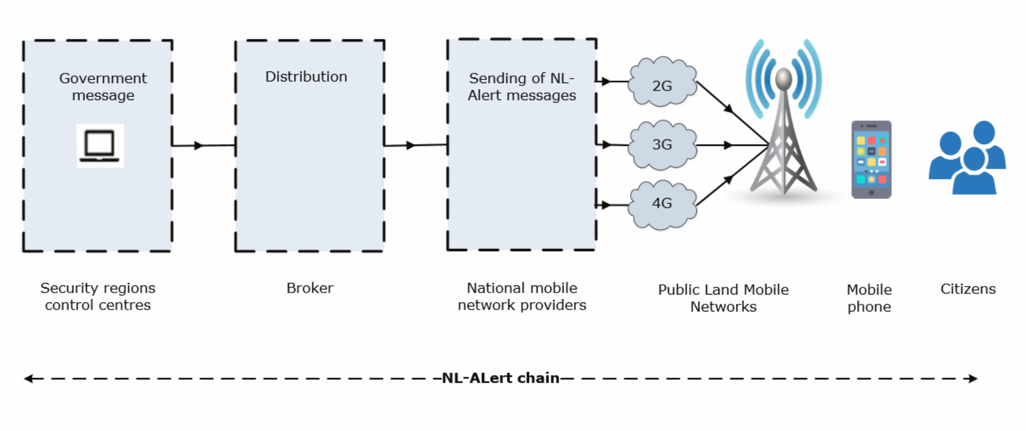
Government message
Distribution
Sending of NL-Alert messages
2G
3G
4G
Security regions control centres
Broker
National mobile network providers
Public Land Mobile Networks
Mobile phone
Citizens
NL-ALert chain

Figure 2. *The NL-Alert chain via the national mobile network providers (source: AT).*

On 24 June 2019, the Utrecht Joint Emergency Response Centre was granted a national account for one day that was authorised to send regional or supraregional NL-Alert messages on behalf of all security regions and their regional control centres upon request. This was done in connection with a software update for the regional control centres and security regions that was rolled out by the police in stages over the course of the day. All security regions and their regional emergency response centres were informed of this at the beginning of June.

Safeguarding of KPN continuity measures

For a number of years, KPN has been embedding continuity measures into its policy by means of *security policies*. Among other matters, these policies distinguish between critical and non-critical services. The voice service is designated as a critical service and hence is subject to the strictest architectural requirements, a maximum downtime standard of four hours and a maximum of 100,000 affected users in the event of simple malfunctions. Furthermore, the network's capacity must be guaranteed during peak hours.

KPN has also implemented measures to safeguard the continuity of NL-Alert and the Cell Broadcast platform. Cell Broadcast is part of the critical Mobile service.

Safeguarding of accessibility to emergency services

Policy: measures, coordination and communication

In response to previous malfunctions within the 112 chain, agreements were developed in 2012 to safeguard public access to the emergency services in the event of planned or unplanned circumstances. These agreements were then implemented into a set of regulations, which served as the predecessor of the police's Generic Operational Scenarios (OGD). The OGD describes four scenarios relating to malfunctions within the 112 chain and prescribes measures to deal with such situations. The purpose of these measures is to ensure that any emergency

[1] The broker enables the control centre to create and send NL-Alert messages to the mobile network providers

calls - situations in which every second counts - are relayed to the emergency service(s) in question as quickly as possible. Scenario 4 in the OGD is the closest match to the situation on 24 June 2019 and describes one concrete measure that emergency services can take: '*Staff all police stations and fire stations*.' However, responsibility for this measure is partly borne by the security regions (staffing fire stations).

Following the malfunctions in 2012, IJ&V and AT initiated an investigation. Based on this investigation, recommendations were made to offer citizens greater perspective for action in the event of inaccessibility of the 112 emergency services. The Minister of Justice and Security adopted the recommendations stemming from the investigations and formulated a perspective for action and agreements relating to communication with citizens as part of a letter to the Dutch Lower House of Parliament. Following up on this letter to Parliament, the Ministry of Justice and Security sent a letter to the head of the police, the chairs and directors of the security regions, the regional fire brigade commanders and the directors of the RAVs in June 2013. Among other matters, this letter described the specific perspective for action that would be communicated to citizens in the event of a breakdown of the 112 emergency services. This perspective for action includes three options in the event that the 112 emergency services is temporarily less accessible or completely inaccessible[2]. The police and security regions must be able to use this perspective for action to determine the measures that they must take. Clear information is lacking in relation to which aid stations they must staff and open up.

The security regions were not involved in the perspective for action specified in the OGD and the June 2013 letter from the Ministry of Justice and Security. These documents do not contain any agreements concerning methods of communication between the Ministry of Justice and Security, the police and the 25 security regions or the distribution of roles and responsibilities between these parties. It is vitally important that agreements such as these are made as the Ministry of Justice and Security is responsible for communication and the other organisations are responsible for the execution of the measures.

The NL-Alert Implementation and Policy Framework applicable on 24 June 2019 specified that a national NL-Alert can be issued in the event that crisis management has been scaled up to the national level[3]. In situations such as the inaccessibility of 112, the Ministry of Justice and Security must provide the security regions with a uniform national message accompanied by a perspective for action. The description does not specify how the many parties involved must do this in practice in order to ensure quick and simple communication to citizens. Following the events of 24 June 2019, the Ministry of Justice and Security added an appendix to the NL-Alert Implementation and Policy Framework that specifically addresses how a national NL-Alert should be sent in the event of serious disruption to the 112 emergency services[4]. The inaccessibility of the 112 emergency services presumably will not be the last incident that causes social unrest or disruption. As yet, the amended NL-

[2] If the citizen makes a call from a land line and no connection is made, then he/she must call via a mobile phone and vice versa. If all telephone facilities are non-functional, then the citizen must go to the nearest station/office of the emergency service in question.

[3] NL-Alert Implementation and Policy Framework, 1 January 2019. The Ministry of Justice and Security.

[4] 'Procedure for sending of NL-Alert by the Ministry of Justice and Security in the event of a serious disruption of 1-1-2 services', November 2019 Ministry of Justice and Security.

Alert Implementation and Policy Framework still lacks a general procedure that would apply in the event of incidents involving nationwide impact.

With regard to communication, the OGD and the Ministry's June 2013 letter both specify who is in charge of communication with citizens: the Ministry of Justice and Security. In addition, scenario 4 from the OGD contains a clear message to send to the citizens. However, the message specified in the letter from the Ministry of Justice and Security is insufficiently concrete as it does not make clear what options are open to citizens in the event of the inaccessibility of the 112 emergency services.

Implementation of policy by the various organisations

The perspective for action from the Ministry of Justice and Security's June 2013 letter has been published on the websites of the security regions and the website of the Ministry of Justice and Security. It is clearly evident that by December 2019, a number of websites were still announcing that the 112 emergency services has always been accessible.

Within the security regions and the Ministry of Justice and Security, there has been little to no operationalisation of the implementation measures stemming from the perspective for action (as described in the Ministry of Justice and Security's June 2013 letter) into agreements and/or procedures for the crisis response organisations. In addition, the Ministry of Justice and Security - which has a substantial interest in the organisations following the policy - has neglected to verify whether the organisations have complied with the letter dated 13 June 2013.

1.3.2 The malfunctions and the resulting actions taken by the organisations responsible

KPN

At 15:32 on Monday 24 June 2019, the first report of a decline in visible traffic was received by KPN's monitoring centre. This report was followed by numerous others. Based on these reports, as well as responses from customers and KPN's own organisation, KPN initiated the emergency procedure. At 17:45, the investigative team identified the cause of the malfunction, at 18:30, the first system was successfully restarted and by 18:52, the voice service - and hence the public safety answer point 112 - was once again fully accessible.

After the first regional NL-Alert message - and some time later the first national NL-Alert message - had been sent, the first signs began to emerge via social media and from within the government that the NL-Alert messages sent via the KPN network had not been received. On Monday evening, an official logged in and examined the reporting function. When doing so, no alerts were visible on the Cell Broadcast platform. The next day, an investigation was initiated and at 11:30, it was found that a problem had been caused by a previous configuration change. This problem had been resolved by 11:40, at which point the NL-Alert service via 4G became available again.

Government and emergency services

Following identification of the malfunction, the police acted in compliance with scenario 4 of the OGD. During the inaccessibility of the 112 emergency services on 24 June 2019, scenario 4 - in which the public safety answer point 112 is inaccessible due to a malfunction of public infrastructure or the technical 112 facility - is the most appropriate of the OGD scenarios, although it did not match the actual situation exactly. Scenario 4 assumes that the national police hotline 0900-8844 is operational, although on 24 June 2019, this was not the case due to the malfunction of the KPN telephone network. In compliance with scenario 4, the police thoroughly examined the situation and provided information to the regional emergency response centres. Subsequently, they informed the police management team and advised the Ministry of Justice and Security to send a national NL-Alert message. The Ministry of Justice and Security chose to wait before sending a uniform national message containing information about the malfunction and notification of the fact that citizens can visit police stations and fire stations in the event of any emergency. As the service number 0900-8844 was also inaccessible, the Ministry of Justice and Security wanted to offer citizens a broader perspective for action. However, the Ministry's decision to delay sending clear information to citizens meant it lost control of the response to the crisis. The lack of a uniform national message resulted in a huge volume of regional NL-Alert messages, which in turn caused other malfunctions in the NL-Alert technical chain. This incident was separate from the NL-Alert malfunction at KPN.

As the security regions had little to no access to plans and/or procedures addressing inaccessibility of the 112 emergency services or a corresponding perspective for action, a number of security regions were forced to play catch-up once the police published a message on Twitter informing citizens that they could report emergencies to fire stations. This is because a number of security regions had decided not to staff the fire stations, opting instead to offer other alternative measures. The security regions eventually did implement the measures specified in the OGD and the June 2013 letter from the Ministry of Justice and Security. They also implemented additional measures and provided information to citizens about the malfunction and alternative ways to contact the emergency services.

Care organisations

Less urgent reports

In response to the KPN malfunctions, IGJ asked care organisations to report less urgent situations in addition to the mandatory emergency reports, which may have resulted in delay to healthcare provision. This request was made as a result of media reports, among other factors. This information gave IGJ greater insight into the situations and allowed them to answer questions from professionals in greater detail.

Reports by professionals

In the period following the malfunction, IGJ received no emergency reports, although it did receive four messages from care organisations regarding the consequences of the inaccessibility of the 112 emergency services and the malfunction at KPN. Three RAVs reported a death during the period of inaccessibility of the 112 emergency services. Due to the inaccessibility, the RAVs could not be reached on time. The RAVs reported that their responses to the incidents were within the standard time limits and in compliance with protocols.

IGJ deeply regrets the deaths of the three citizens during the period of inaccessibility of the 112 emergency services. Whether the delayed initiation of paramedic assistance played a role in the deaths of the parties in question cannot be established by IGJ.

A fourth RAV reported another critical situation involving a delayed alert to the RAV.

Alerts resulting in an additional internal investigation
Furthermore, IGJ also received two alerts for which they asked the organisations involved to conduct an internal investigation. A hospital reported that the transfer of a patient for an urgent procedure in another hospital was delayed by 20 minutes as a result of the malfunction of KPN's telephone network. This hospital investigated the incident and the specialists in question found that the delay had no direct consequences for the patient. However, the incident did allow lessons to be learned for future knowledge expansion concerning the internal crisis response organisation and readiness to use the Emergency Communication System (NCV)[5]. The second report concerned a complaint from a GP regarding the admittance of a patient to hospital during the malfunction of the KPN telephone service. The hospital investigated the complaint and worked with the GP to identify a number of points for improvement in order to prevent the problems from recurring. The incident did not cause any harm to the patient.

Reports by citizens/care recipients
During the period subsequent to the inaccessibility of the 112 emergency services and the malfunction at KPN, the National Healthcare Control Centre - part of IGJ - did not receive any questions or complaints regarding the quality of care.

Survey
The following experiences were identified by the short survey issued by IGJ to the RAVs, HAPs and GHORs in order to gain insight into how these organisations dealt with the inaccessibility of the 112 emergency services and the voice service malfunction:

Half of the RAVs operated in accordance with a scenario playbook in order to mitigate the inaccessibility of the 112 emergency services. They also indicated that the majority of these playbooks were insufficient. These playbooks mainly focused on the regional level with neighbouring regions taking over tasks, and no scenario was included that involved national inaccessibility of the 112 emergency services. The RAVs indicated that no national strategy or information provision structure was in place. They also observed that chain partners such as hospitals were not sufficiently aware of the NCV.

Many RAVs that operated without a scenario playbook said that they sufficiently mitigated the inaccessibility of the 112 emergency services by means of improvisation, such as increasing visibility by stationing an ambulance outside HAPs. Problems in this regard included the lack of alternative communication facilities as a backup and a lack of clarity concerning the management of a number of ambulance response centres (MKAs).

[5] The NCV is a separate telecommunications network that is specifically intended for the use of the government and critical parties in the event of disasters or crisis in the Netherlands involving overloading of or disruption to the public fixed-line telephone network. The network is robust enough to be used in situations such as power cuts, floods and disruptions to telephone services.

The HAPs affected by the KPN telephone malfunction were unable to receive incoming phone calls. Outgoing phone calls to the MKAs or hospitals also proved impossible. Practically all of the HAPs had a scenario addressing disruption of telephone services. In the majority of cases, it was not possible to comply fully with the scenario playbook as it did not include scenarios involving a national malfunction of telephone services. This was due to the fact that all of the emergency situations were based on the KPN network functioning as a backup system.

In general, the consequences stemming from the malfunction of the voice services were sufficiently resolved within the HAPs by using alternative telecommunication resources, deploying extra staff and maintaining short lines of communication within the HAPs. The HAPs indicated that they are not connected to the NCV and are insufficiently aware of its existence. There is also insufficient awareness of alternative emergency numbers and other numbers.

During the crisis, the GHORs played a coordinating role to ensure sufficient continuity of care in the region. For this purpose, the GHORs investigated whether the chain partners (e.g. hospitals, GPs and obstetricians) had been affected by the inaccessibility of the 112 emergency services and the KPN malfunction. The GHORs provided information to these organisations and monitored whether any problems were created. During this process, the GHORs often observed that the chain partners were able to implement sufficient measures themselves. Around half of the GHORs used a scenario playbook to mitigate the malfunction of KPN's voice services.

Some GHORs mentioned that the continuity plan applicable in the security region in question states that the inaccessibility of the 112 emergency services does not affect the activities of the GHOR and that the control measures were not applicable. However, this was found to be incorrect. A variety of measures focusing on the chain partners were implemented by the GHORs. A number of other GHORs indicated that they roughly followed the instructions specified in the malfunction/disruption of telephone services document, but that the reality of the situation always differs from the prior expectations. Even unplanned alternatives that were spontaneously improvised at the time of the malfunction, such as Skype or WhatsApp calls, worked faster than using the NCV. Some GHORs that did not operate in accordance with a scenario playbook emphasised that disasters and crises do not follow scripts and that attentive, resilient and competent response organisations must be established that can cope with any situation. Others reported that they used the NCV but encountered problems while doing so, for example, due to unfamiliarity with the system among the staff. It also became apparent that some operational GHOR staff could not be reached by phone and that no incoming or outgoing calls to or from the MKAs were possible.

1.3.3 Causes of the malfunctions and subsequent mitigation measures

Causes of KPN malfunctions

Inaccessibility of the 112 emergency services and the malfunction of the voice service

The cause of the malfunction was the failure of the call routing platform: an essential component of KPN's telephone network. The call routing platform is essential to ensure every phone call is put through to the correct connection, including calls to 112. This call routing platform consists of four independently operating call routing systems. The failure was caused by a software configuration problem affecting the four call routing systems in combination with the synchronous operation of these systems. A problem with the counters resulted in a large volume of error messages, which the system automatically stores. Every new call routing request resulted in a new error message. The storage of this substantial volume of error messages in combination with the huge number of call routing requests due to repeat traffic meant that after an hour, the call routing platform was no longer able to process the call routing requests.

In addition to this direct cause, a number of other causes and circumstances were also partly to blame for the disruption of voice services and the inaccessibility of the 112 emergency services. For example, in June 2018, KPN decided to use the call routing platform for the routing of 112 call traffic in connection with a scheduled upgrade of the 112 platform. The failure of the call routing platform on 24 June 2019 meant that call routing information could no longer be provided, which resulted in the inaccessibility of the public safety answer point 112.

In addition, a change to the software used by the call routing platform's service management system had unintentionally caused the counters of the four call routing systems - which monitor the number of call routing requests - to run synchronously. For this reason, on 24 June 2019, the four counters reached a negative value at virtually the same time. The large volume of error messages stemming from this chain of events ultimately resulted in the failure of the call routing platform.

Finally, in January 2019, an error was made when implementing a script intended to issue a warning in the event that the counters reach 95% of their maximum value. As a result, the counters were not reset in a timely manner, which resulted in them registering a negative value. The interplay between these causes and circumstances caused that the redundancy of the system was not beneficial anymore.

NL-Alert malfunction

For the purposes of the legal obligation to provide a 4G report for NL-Alert, a configuration change had to be carried out on the KPN Cell Broadcast platform at 10:30 on the day in question. At 12 noon, a periodic network scan was conducted to examine the status of the cellular radio network . The combined effects of the configuration change and the network scan caused the 4G adapter of the Cell Broadcast platform to overload. From that moment onwards, KPN was no longer able to process NL-Alert messages via the 4G network.

After the first regional NL-Alert message - and some time later the first national NL-Alert message - had been sent, the first signs began to emerge via social media and from within the Dutch government that the NL-Alert messages sent via the KPN network had not been received. On Monday evening, an official logged in and examined the reporting function. When doing so, no alerts were visible on the Cell Broadcast platform. The next day, an investigation was initiated and at 11:30, it was found that a problem had been caused by a previous configuration change. This problem had been resolved by 11:40, at which point the NL-Alert service via 4G became available again.

Measures taken by KPN

Immediately following the malfunction, KPN implemented measures to prevent recurrence of the situation and to boost the resilience and reliability of the voice service and the 112 call routing system. For this purpose, KPN carried out a root cause analysis and an extensive evaluation of the malfunction, as well as commissioning an investigation by Bell Labs Consultancy. In August 2019, based on the findings of these investigations, KPN formulated an action plan to implement the other measures as quickly as possible.

The majority of these measures have since been implemented. One of the measures intended to prevent recurrence of the situation involves adjusting the software configuration of the four call routing systems. This adjustment will prevent call routing requests from being disrupted as a result of large volumes of error messages. In addition, the resilience of the call routing system for 112 traffic has been improved by quickly rerouting 112 traffic to the public safety answer point 112 via alternative channels in the event the call routing platform starts to operate slowly or ceases to operate altogether.

Immediately following the NL-Alert malfunction, KPN implemented a number of measures to prevent a recurrence of the problem. The majority of these measures have since been implemented. One of these measures is the inclusion of a network scan in the test environment. In collaboration with the supplier, KPN has established extra alerts for the purposes of monitoring the Cell Broadcast platform in order to enable timely detection of similar malfunctions.

The malfunction of the NL-Alert service on the Cell Broadcast platform was included in KPN's evaluation of the malfunction of the 112 emergency services and the telephone network.

1.4 Conclusions

Radiocommunications Agency Netherlands (AT)

Following its investigation, AT concluded that implementation of the measures recorded in the action plan would help ensure a more robust 112 emergency services and telephone network and minimise the risk of recurrence of a malfunction such as the one that occurred on 24 June 2019. Based on the malfunctions, KPN has already implemented a number of important and appropriate measures in relation to the 112 emergency services, the telephone network and the NL-Alert system.

AT has drawn the following conclusions based on the findings of its investigation into the inaccessibility of the 112 emergency services and the voice service malfunction:

- The resilience of the 112 call routing system has been boosted following implementation of measures from the action plan.
- Insufficient attention was paid to the impact of planned and unplanned vulnerabilities within the call routing platform's software configuration.
- Within the critical voice and 112 emergency services, too little attention was paid to ensuring the resilience of the system in the event of changes.
- Lessons stemming from the root cause analysis and the evaluation process for 112 and the voice service have been adequately learned.
- There was insufficient exchange of specific performance indicators between the network elements that prevent overload.
- There was a lack of end-to-end service management in the 112 chain.
- There was insufficient discipline in the process in a number of areas.

AT has drawn the following conclusions based on the findings of its investigation into the NL-Alert malfunction:

- KPN failed to detect the NL-Alert malfunction caused by the Cell Broadcast platform on the 4G network within a sufficient time frame.
- The NL-Alert service was not treated as a separate critical service within KPN.

Furthermore, AT's investigation found that KPN was in compliance with the legal obligations relating to continuity as specified in Article 7.7(3) and Chapter 11a of the Telecommunications Act (Telecommunicatiewet). However, the malfunction occurred despite KPN's compliance with the legal requirements. High-impact malfunctions cannot always be prevented as not every situation is conceivable in advance.

The Inspectorate of Justice and Security (IJ&V)

IJ&V has come to the following conclusions based on the findings of its investigation:

- During the malfunction, a great deal of action was taken by the emergency services to ensure the accessibility and availability of their services and to provide all necessary assistance to the public.
- The documents (the ODG and the Ministry of Justice and Security's letter dated June 2013) relating to the inaccessibility of the 112 service were not sufficiently fleshed out.
- The Ministry of Justice and Security and many of the security regions lack knowledge of documentation providing scope for action in the event of a crisis involving inaccessibility of the 112 emergency services. It was also found that these policy documents have been neither implemented nor operationalised.
- The Ministry of Justice and Security had insufficient control of the implementation of the policy specified in the letter sent to the parties involved in June 2013.
- The Ministry of Justice and Security also lacked direct control of the communication process during the crisis.

The Health and Youth Care Inspectorate (IGJ)

IGJ has come to the following conclusions based on the findings of its investigation:

- There was a great deal of cooperation between the care organisations. These organisations sufficiently resolved the problems using a substantial degree of resourcefulness.
- The care organisations examined during the investigation mitigated the consequences of the voice service malfunction by deploying extra staff and alternative telecommunication resources.
- The scenario playbooks did not anticipate a situation involving national inaccessibility of the 112 emergency services and a national malfunction of the voice service.
- The backup system NCV proved insufficient due to widespread unfamiliarity with the system.

1.5 Recommendations

Based on these conclusions, it is clear that further improvement and professionalisation is necessary within the organisations involved. In order to achieve this, the following recommendations have been made based on each of the separate investigations.

Radiocommunications Agency Netherlands (AT)

AT has issued the following recommendations:

To KPN:

- Implement the measures specified in the action plan in accordance with the schedule in order to boost the resilience of the 112 emergency services and the telephone network and minimise the risk of the malfunction recurring.
- Specify the 112 chain and the NL-Alert service as independent items on the list of critical services in order to further highlight the urgent need for continuity of these critical public services.
- Implement organisational and technical measures to prevent or minimise the impact of software errors or configuration errors, partly in anticipation of the increasing levels of virtualisation of networks and services.
- Ensure a solid risk inventory in order to identify, mitigate or resolve risks in the event that services and platforms are adjusted or phased out.

To the Ministry of Justice and Security:

- Enable continual testing and monitoring of 112 calls throughout the entire 112 chain. Within the current TDM telephone network, KPN continually tests 112 call routing using a call generator. No such testing method is available for the mobile telephone network. This testing method was removed following implementation of the upgraded 112 platform.
- Enable continuous testing and monitoring of NL-Alert without causing disruption to users. NL-Alert sends test messages twice a year. However, there is no option that enables continual testing of the NL-Alert chain without it being noticeable to users.
- In the event of any future decisions concerning alternative structures to or tendering processes within the current 112 chain, attention should be paid to the integral control and organisational aspects (in addition to just the technical aspects) in order to minimise risks in the chain.

To the telecom sector:

- Proactively identify new weaknesses and dependencies in the architecture, technology and software in order to mitigate or resolve them. In this regard, pay specific attention to the dependencies of operational systems, database connections, configuration adjustments, software updates and identical software.

As part of its regular monitoring duties, AT will examine KPN's compliance with the legal obligations applicable to the necessary and appropriate measures (both those already implemented and those yet to be implemented). AT wants to receive periodic progress reports relating to the action plan and the implementation of the recommendations.

The Inspectorate of Justice and Security (IJ&V)

IJ&V has issued the following recommendations:

To the Ministry of Justice and Security, the police and the 25 security regions:

- Work together to ensure further elaboration of policy governing inaccessibility of the 112 emergency services.
- Ensure the documents are implemented into the organisations involved (in this case, the Ministry of Justice and Security, the police and the 25 security regions) and ensure the staff are familiar with the documents.

To the Ministry of Justice and Security and the 25 security regions:

The NL-Alert Implementation and Policy Framework has been amended since the events of 24 June 2019. A specific procedure has been added to the framework that addresses national malfunctions/inaccessibility of the 112 emergency services.

- Expand this procedure in order to make it generally applicable to all incidents involving national impact.

To the Ministry of Justice and Security:

- Monitor the implementation of policy into the organisations involved.

To the Ministry of Justice and Security, the police and the 25 security regions:

- Ensure all parties operate in compliance with the agreements made.

The Health and Youth Care Inspectorate (IGJ)

IGJ has issued the following recommendations:

Although the staff showed great resourcefulness during the crisis, it is essential that lessons are properly learned. It is equally vital that professionals know how to contact each other in crisis situations.

To the HAPs and hospitals:

- Ensure the NCV can be used sufficiently.

To the RAVs, HAPs and GHORs:

- Ensure scenario playbooks that include a strategy in the event of national inaccessibility of the 112 emergency services and a malfunction of the national telephone system, and coordinate these playbooks with other organisations involved.

Follow-up action for IGJ:
During its regular process of monitoring the care organisations involved, IGJ will test whether the scenario playbooks have been amended and whether sufficient capability to use the NCV has been ensured.

The implementation of the recommendations will be monitored by the various inspectorates in accordance with their particular supervisory area.

Mission of the Inspectorate of Justice and Security

*The Inspectorate of Justice and Security monitors the domain of justice and security
in the interest of society, the parties subject to monitoring and persons politically and administratively responsible,
in order to provide insight into the quality of the performance of tasks and the compliance with rules and standards,
to detect risks
and to stimulate organisations to perform better,
thereby contributing to a just and safe society.*

Mission of the Agentschap Telecom

The Radio Communications Agency ensures the availability and reliability of the IT and communication networks, to make sure that the Netherlands is safe and connected.

Mission of the Inspectie Gezondheidszorg en Jeugd

Everyone in the Netherlands should be able to rely on good healthcare and youth care. The kind of care that you would want for yourself and your loved ones, in every situation and throughout every phase of life. Our role is to supervise healthcare and youth care services in the Netherlands and the international market for medicines and medical devices. Basically we have confidence in the providence of healthcare and youth care services. Yet, if necessary we will intervene.

This is a publication of:
Inspectorate of Justice and Security
Ministry of Justice and Security
Turfmarkt 147 | 2511 DP The Hague | The Netherlands
PO Box 20301 | 2500 EH The Hague | The Netherlands
Contact form | www.inspectie-jenv.nl/english

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
Emmasingel 1 | 9726 AH Groningen
Postbus 450 | 9700 AL Groningen
www.agentschaptelecom.nl

Inspectie Gezondheidszorg en Jeugd
Ministerie van Volksgezondheid, Welzijn en Sport
Stadsplateau 1 | 3521 AZ Utrecht
Postbus 2518 | 6401 DA Heerlen
www.igj.nl