Belgisch Instituut voor
postdiensten en telecommunicatie

Rapport définitif du Conseil de l'IBPT du 14 septembre 2020 concernant l'incident chez Proximus le 5 avril 2019

VERSION NON CONFIDENTIELLE

Institut belge des services postaux et des télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 | 1030 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

Synthèse

1. Le 5 avril 2019, un incident technique s'est produit chez Proximus, empêchant qu'une grande partie des appels vocaux vers et depuis Proximus ait lieu.

2. Cet incident était causé par une défaillance technique logicielle qui, en raison d'une combinaison de circonstances, a engendré une défaillance d'une composante essentielle du réseau.

3. Le jour même, Proximus a pris quelques mesures techniques provisoires afin que la défaillance logicielle ne se produise plus. Une solution permanente a ensuite été mise en œuvre lors des semaines suivantes.

1. Introduction

4. Le présent rapport constitue une analyse de l'incident du 5 avril 2019 sur le réseau de Proximus. En raison d'une défaillance d'un élément de réseau essentiel, la communication entre le réseau fixe de Proximus et d'autres réseaux était temporairement impossible. En conséquence, les services d'urgences n'étaient également disponibles que de manière limitée lors de l'incident.

5. La présente analyse comprend tant le cadre juridique, que le traitement lors de l'incident et la cause technique sous-jacente. Lors de la période suivant l'incident, diverses mesures avaient déjà été prises pour éviter que des événements semblables se produisent. Celles-ci sont également décrites dans le présent rapport. Enfin, le rapport contient quelques propositions de recommandations et la réaction de Proximus quant à ces dernières.

2. Cadre juridique

6. En vertu de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la « LCE »), l'IBPT peut contrôler si Proximus prend des mesures (préventives) pour garantir un accès ininterrompu aux services d'urgence (article 107).

7. L'IBPT peut contrôler si Proximus prend des mesures (préventives) pour gérer le risque en matière de sécurité de ses réseaux et services de manière appropriée et pour réduire au maximum les conséquences des incidents de sécurité pour les utilisateurs et les réseaux interconnectés (article, § 1er, de la LCE) et peut donner des instructions contraignantes à cet égard (article 114/2 de la LCE).

8. En vertu de la loi du 1er juillet 2011relative à la sécurité et la protection des infrastructures critiques et en sa qualité de service d'inspection pour le secteur des communications électroniques, l'IBPT peut contrôler si le plan de sécurité de l'exploitant (PSE), en l'occurrence Proximus, contient effectivement les mesures visant à prévenir, à atténuer et à neutraliser le risque qui s'est produit lors de l'incident du 5 avril 2019 (article 13, § 1er) et si Proximus actualise sont PSE lorsque nécessaire (article 13, § 6).

3. Historique

3.1. Événements du 5 avril 2019

9. Le vendredi 5 avril 2019 à 15h30, le réseau fixe de Proximus a été isolé en raison d'un problème technique au niveau d'une composante essentielle pour le trafic interréseaux. En conséquence, aucune communication n'avait lieu entre le réseau fixe de Proximus et le réseau mobile de Proximus. La communication entre le réseau fixe de Proximus et les réseaux, tant fixes que mobiles, d'autres opérateurs n'était plus possible non plus. Ce problème technique a également eu pour effet de fortement limiter l'accessibilité téléphonique des services d'urgence. Seuls les appareils connectés au réseau fixe de Proximus pouvaient encore contacter les services d'urgence par téléphone. Le tableau de Proximus ci-dessous représente graphiquement l'impact sur les services de téléphonie. L'impact du problème était limité à la téléphonie. Les SMS et l'accès à Internet, tant fixe que mobile, n'ont pas été touchés. Ainsi, les services d'urgence restaient accessibles pour les utilisateurs d'appareils mobiles par SMS via le numéro 8112, à savoir le numéro réservé en temps normal aux sourds et malentendants exclusivement.

	TO							
FROM	100-101-112	PXS Fix	Scarlet Fix	PXS ISDN	PXS Mob	OLO	MOLO	BICS
PXS Fix	OK	OK	OK	NOK	NOK	NOK	NOK	NOK
Scarlet Fix	OK	OK	OK	NOK	NOK	NOK	NOK	NOK
PXS ISDN	NOK	NOK	NOK	NOK	NOK	NOK	NOK	NOK
PXS Mob	NOK	NOK	NOK	NOK	OK	OK	OK	OK
OLO	NOK	NOK	NOK	NOK	OK	OK	OK	OK
MOLO	NOK	NOK	NOK	NOK	OK	OK	OK	OK
BICS	NOK	NOK	NOK	NOK	Ok	OK	OK	OK

10. À 16h05, Proximus a informé la permanence de l'IBPT de la situation. La permanence a ensuite averti le centre de crise. Le centre de crise avait entre-temps déjà été informé de la présence de problèmes par les centrales d'urgence. Les membres du personnel du service NetSec qui étaient encore présents à ce moment-là dans les locaux de l'IBPT ont aidé la permanence avec la coordination de la communication entre le centre de crise, Proximus, Telenet, Orange et Voo. Vu la nature et l'impact de l'incident, les clients des autres opérateurs ont également été touchés indirectement.

11. À 17h51, les problèmes chez Proximus étaient toujours en cours et aucune déclaration ne pouvait encore être faite quant à une éventuelle solution et le moment à partir duquel elle allait pouvoir être appliquée. Pour cette raison, le centre de crise avait invité les services publics concernés à une réunion de crise à 18h45. L'IBPT a envoyé un officier de liaison au centre de crise et a également envoyé un représentant de l'IBPT chez Proximus pour pouvoir suivre la situation de près.

12. À 18h15, le problème pour les services d'urgence était résolu. Cela n'a toutefois pas pu être confirmé à ce moment-là, et cette heure n'a été confirmée qu'après l'incident.

13. Aux alentours de 18h45, le centre de crise a signalé que quelques centrales d'urgence indiquaient que les problèmes semblaient résolus. Cela ne pouvait pas être confirmé par Proximus à ce moment-là.

14. À 18h50, le problème était en grande partie résolu pour tous les types d'appels. Cela n'a toutefois pas pu être confirmé à ce moment-là, et cette heure n'a été confirmée qu'après l'incident.

15. À 18h51, toutes les centrales d'urgence ont confirmé que l'accès téléphonique au numéro d'urgence 112 semblait fonctionner correctement. Toutefois, cela ne peut à nouveau pas être confirmé par Proximus.

16. À 19h, le centre de crise lance la phase fédérale.

17. À 19h, une nouvelle réunion de la cellule de crise commence chez Proximus, à laquelle assiste le représentant de l'IBPT. Lors de la réunion, il est confirmé que la situation s'améliore en effet et que la capacité augmente de façon systématique. Étant donné que les appels d'urgence reçoivent la priorité sur le réseau de Proximus, les centrales d'urgence étaient en effet les premières à remarquer l'amélioration de la situation.

18. À 19h54, les centrales d'urgence d'Anvers et de Flandre-Orientale signalaient à nouveau des problèmes.

19. À 20h14, Proximus confirmait l'existence de quelques problèmes résiduels, en conséquence des événements survenus plus tôt cette journée. Toutes les interconnexions avec les différents opérateurs ne fonctionnent ainsi pas encore à pleine capacité, des appels pouvaient encore échouer. Ces problèmes seront progressivement résolus dans l'heure qui suit.

20. À 20h22, le centre de crise mettait fin à la phase fédérale.

21. À 21h25, Proximus confirmait que tous les problèmes résiduels avaient été résolus. La situation était revenue complètement à la normale.

3.2. Événements après le 5 avril 2019

22. Lors du week-end des 6 et 7 avril, Proximus a surveillé son réseau de plus près. Plus aucun problème n'a été détecté.

23. Le mardi 9 avril, Proximus a fourni à l'IBPT un rapport succinct sur les événements du 5 avril. Proximus y donnait un aperçu des mesures temporaires prises par l'opérateur le 5 avril pour que la situation revienne à la normale. En outre, Proximus a indiqué que Nokia, le fournisseur de la composante de réseau défaillante, développait une solution permanente. Cette solution sera installée lors des nuits du 17 et 18 avril.

24. Le vendredi 12 avril 2019, une réunion a été organisée à l'IBPT afin de discuter de la cause du problème du 5 avril. Des représentants de Proximus, de l'IBPT, du SPF Économie, du SPF Santé publique, de la Direction 112 et d'ASTRID ont participé à la réunion. Lors de celle-ci, Proximus a donné plus d'explications sur la cause de l'incident. Il s'agissait d'un bug logiciel qui est apparu à la suite d'une combinaison de facteurs. Vu que la situation sur les différents systèmes redondants était identique, ce bug a provoqué une défaillance simultanée des différents systèmes, supprimant ainsi toute redondance.

25. Le 24 avril 2019, le Conseil de l'IBPT a entendu Proximus concernant les événements du 5 avril. [Confidentiel]

26. Le 6 mai 2019, une réunion a été organisée à l'IBPT afin de discuter de futures améliorations potentielles. Des représentants de Proximus, de l'IBPT, du SPF Économie, du SPF Santé publique, de la Direction 112, du centre de crise et d'ASTRID ont participé à la réunion. Proximus a proposé quelques solutions techniques pour éviter l'apparition d'un incident similaire à l'avenir. Les différentes parties devaient analyser l'impact de ces solutions et communiquer le résultat à l'IBPT pour le 7 juin 2019. L'IBPT contacterait les autres opérateurs pour connaître leur avis concernant les solutions proposées.

27. Le 17 mai 2019, une réunion a été organisée à l'IBPT entre les mêmes parties que celles présentes le 6 mai 2019. La réunion concernait la rédaction d'un plan de communication amélioré en cas d'incidents ayant un impact sur les services d'urgence.

28. Le 14 juin 2019, une réunion de suivi a été organisée à l'IBPT afin de discuter plus en détail des solutions techniques potentielles. ASTRID a présenté ses réflexions concernant les différentes solutions de Proximus, tandis que l'IBPT a présenté l'input d'Orange et de Telenet. Sur cette base, une liste restreinte de solutions a été retenue. Ces solutions seront développées de manière plus détaillée pour le 12 septembre.

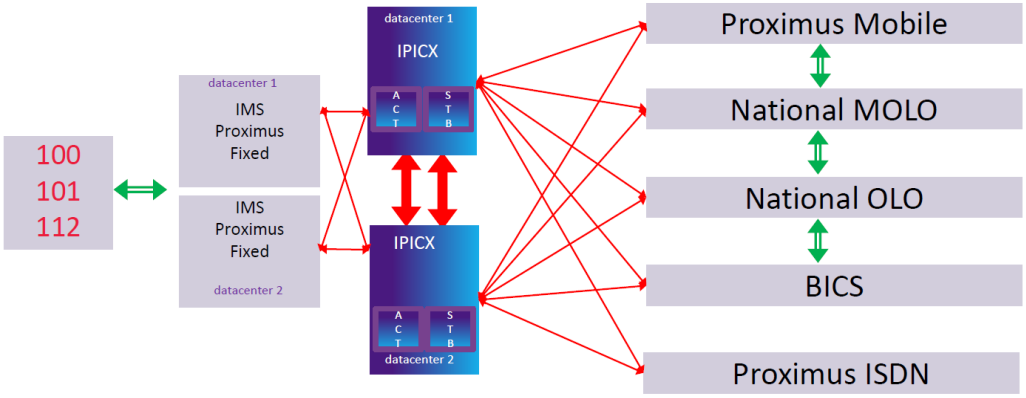
29. Le 22 juillet 2019, l'IBPT a envoyé une première version de cette analyse à Proximus pour commentaire.

30. Le 30 septembre 2019, Proximus a répondu à cette analyse.

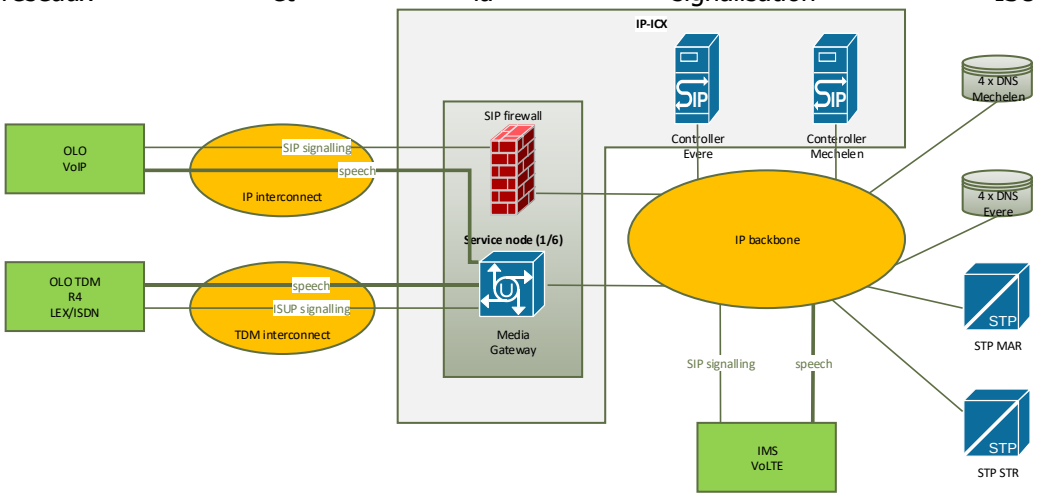
4. Analyse technique

4.1. Cause

31. La cause principale de l'incident du 5 avril résidait dans une erreur logicielle de la plateforme IPICX de Proximus. Il s'agit de la plateforme qui connecte les différents réseaux de téléphonie de Proximus avec les réseaux d'autres opérateurs. Un dysfonctionnement de cette plateforme a un impact sur les appels téléphoniques depuis et vers les réseaux de Proximus. La figure ci-dessous montre la position schématique de la plateforme IPIXC de Proximus par rapport aux différents réseaux qui y sont connectés. Le réseau de téléphonie fixe de Proximus se trouve du côté gauche de la figure. Tous les autres réseaux connectés à la plateforme se trouvent du côté droit.



32. La plateforme IPICX est constituée de plusieurs composantes, comme indiqué dans la figure ci-dessous. La cause de l'incident du 5 avril se situait au niveau des *media gateway controllers*. Ceux-ci sont responsables du transport des appels vocaux entre les différents réseaux et la signalisation ISUP.



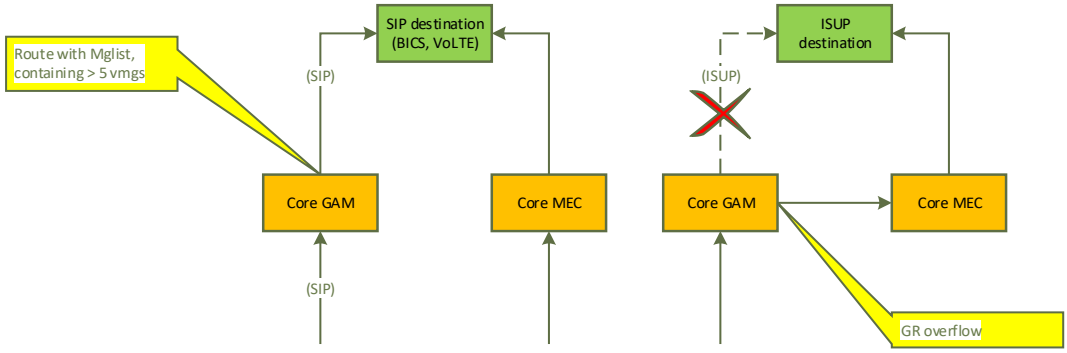
33. Les *media gateway controllers* contenaient une erreur logicielle qui, en raison de circonstances particulières, a provoqué un redémarrage. Lors d'un redémarrage, le gateway est temporairement indisponible. Cela ne constitue pas un problème dans des circonstances normales. En effet, une redondance suffisante est prévue, tant au niveau local que géographique. Étant donné que les circonstances au 5 avril étaient identiques

pour tous les *media gateway controllers*, ils ont tous redémarré au même moment et continuellement. En conséquence de cela, les *media gateway controllers*, et ainsi la totalité de la plateforme IPICX, n'étaient pas fonctionnels pendant l'incident.

34. L'erreur logicielle s'est produite en raison d'une combinaison de 3 facteurs.

35. Une première condition pour l'apparition de l'erreur logicielle est la présence de trafic vocal par IP (au lieu de TDM exclusivement). C'est ce qui s'est passé le 5 avril au niveau des interconnexions avec BICS et Nethys. Quelques semaines auparavant, Proximus avait activé le trafic vocal par IP en tant que partie de leur migration à long terme de TDM vers IP. Cette modification du réseau était donc indirectement l'une des causes de l'incident.

36. Une deuxième condition est la présence de trafic *intercore* entre les différents *media gateway controllers* de la plateforme IPICX. Le trafic *intercore* est le trafic de signalisation qui se produit entre les différents *media gateway controllers* lorsque la remise d'un appel à un partenaire interconnecté échoue via l'un des gateways. Dans ce cas, Proximus transférera l'appel à un autre *media gateway controller* dans un autre centre de données qui est également connecté au même partenaire interconnecté. En d'autres termes, le trafic ne passe pas uniquement *via* les *media gateway controllers*, mais aussi *entre* les *media gateway controllers* dans les différents centres de données. La figure ci-dessous illustre cette situation.



37. Le 5 avril, aux alentours de 15h25, l'opérateur français OVH a rencontré des problèmes avec l'une de ses composantes de réseau. En conséquence, les interconnexions entre Proximus et OVH sont tombées en panne. Les appels qui passaient via la plateforme IPICX de Proximus et étaient destinés à OVH généraient donc du trafic *intercore*. OVH avait en effet une connexion redondante avec la plateforme IPICX. L'on a donc d'abord tenté de délivrer un appel à OVH via une des interconnexions. La tentative a échoué en raison des problèmes chez OVH. Ensuite, l'appel (en tant que trafic intercore) a été transféré vers un autre *media gateway controller* pour tenter une nouvelle fois de délivrer l'appel à OVH, mais sans succès.

38. Les problèmes chez l'opérateur français OVH étaient donc le facteur à l'origine de l'incident du 5 avril. Toutefois, il ne s'agissait pas du seul facteur.

39. La *memory corruption* constituait un troisième facteur pour l'apparition de l'erreur logicielle. En raison d'une gestion de la mémoire défaillante dans les *media gateways*, une opération de lecture ou d'écriture erronée a été effectuée dans la mémoire dans des conditions spécifiques, causées par les deux facteurs précédents. Cela a provoqué le crash de l'un des processus essentiels du *media gateway controller*, entraînant un redémarrage.

40. Les trois facteurs susmentionnés étaient tous les trois nécessaires pour l'apparition de la défaillance. Les deux premiers facteurs, à savoir la présence de trafic IP et de trafic intercore, ne sont pas de mauvais indicateurs. Ce type de trafic est normal et ne devrait pas engendrer de problèmes. En combinaison avec le troisième facteur, cela a provoqué des redémarrages du système, entraînant une défaillance de la plateforme IPICX.

41. Il convient de remarquer que lors des jours précédant le 5 avril, quelques redémarrages occasionnels des *media gateway controllers* avaient été observés. Un ticket « critique » avait alors déjà été ouvert par Proximus auprès de Nokia.

42. Les problèmes résiduels dont il était question à la fin de l'incident étaient causés par les nombreux redémarrages. Étant donné que ces redémarrages ont eu lieu subitement et à de multiples reprises (donc pas d'une manière technique correcte), quelques trunks se trouvaient dans un état non valide, rendant ainsi tout trafic impossible.

4.2. Solution temporaire du 5 avril

43. Le 5 avril 2019, Proximus a rétabli la plateforme IPICX en supprimant deux des facteurs de l'erreur logicielle.

44. L'activation récente de l'autorisation du trafic IP a été annulée. Cela a supprimé le premier facteur de l'erreur logicielle. Seul le trafic TDM était encore possible.

45. La deuxième action entreprise par Proximus était la désactivation du trafic intercore, supprimant ainsi le deuxième facteur de l'erreur logicielle.

46. Concernant le troisième facteur, la *memory corruption*, Proximus ne pouvait réaliser elle-même des modifications. L'erreur résidait en effet dans le *media gateway controller* et non dans l'architecture réseau de Proximus.

47. Les deux mesures prises étaient de nature très temporaire. En effet, normalement ces deux types de trafic devraient être possibles.

48. Les problèmes résiduels ont été résolus en redémarrant manuellement les trunks de manière correcte afin qu'ils aient à nouveau un statut valide et qu'ils puissent transporter le trafic téléphonique.

4.3. Solution provisoire des 17 et 18 avril

49. Après l'incident du 5 avril, Nokia a immédiatement débuté le développement d'un patch pour la cause de l'incident. Le 9 avril, ce patch a été testé dans l'environnement de test de Proximus avec un résultat fructueux.

50. Lors des nuits des 17 et 18 avril, ce patch a été installé dans les systèmes opérationnels de Proximus.

4.4. Solution définitive

51. Ce patch a également été intégré dans la version suivante du logiciel des *media gateway controllers*. Cela évitera que le problème ressurgisse après la prochaine mise à niveau.

5. Recommandations provisoires à Proximus (juillet 2019)

5.1. Recommandations de l'IBPT à Proximus

52. Toute modification du réseau doit être testée en profondeur avant d'être introduite dans l'environnement de production. Il ne suffit pas de tester la modification en isolation. En effet, une modification peut également avoir des répercussions sur d'autres parties du réseau. Par conséquent, toute modification doit être testée dans la mesure du possible de bout en bout dans un environnement le plus proche possible des conditions de l'environnement de production. Lors de ces tests, il ne faut pas uniquement tenir compte des circonstances au sein de son propre réseau, mais également d'autres circonstances (dont la panne ou le comportement anormal de partenaires d'interconnexion).

53. Il est également essentiel de tester régulièrement les systèmes de back-up. En effet, les modifications du réseau peuvent nécessiter des changements au niveau de ces systèmes. Pour éviter de perdre de vue ces modifications, il est conseillé d'effectuer régulièrement une simulation de défaillance de l'une ou plusieurs des composantes du réseau. Cela permet d'évaluer si les systèmes de back-up sont capables de faire face à une panne. Il faut absolument éviter un scénario catastrophe où les systèmes de back-up ne fonctionnent pas parce qu'ils ne sont plus à jour.

54. Le nombre de single-points-of-failure (SPOF) au sein d'un réseau doit être réduit le plus possible. Afin de limiter le risque de défaillance simultanée de composantes ayant la même fonction, il est fortement recommandé de diversifier ces composantes. L'utilisation de composantes de différents fournisseurs pour une même fonction réduit le risque que des circonstances identiques entraînent une défaillance de différents systèmes.

55. S'il n'est pas possible de supprimer un SPOF, il est nécessaire d'établir un business continuity plan (BCP), de sorte qu'en cas de défaillance les mesures nécessaires puissent être prises pour que le réseau continue de fonctionner, même dans un état dégradé.

56. Un planning détaillé doit être réalisé pour chaque mise à niveau ou migration sur le réseau. Ce planning doit, le cas échéant, également être partagé avec les fournisseurs de matériel et de logiciel. Si une mise à niveau a potentiellement un impact important sur le fonctionnement du réseau, les accords nécessaires doivent être conclus avec les fournisseurs afin que ceux-ci puissent agir rapidement en cas d'urgence.

57. Le plan de secours (fallback plan) est un élément essentiel du planning ci-dessus en cas d'échec de la mise à niveau ou de la migration. Ce plan de secours doit contenir des instructions claires et précises en lien avec l'annulation de certaines modifications. Si des problèmes surviennent lors d'une mise à niveau ou d'une migration, les actions nécessaires peuvent alors être entreprises pour résoudre la situation.

5.2. Réaction de Proximus aux recommandations

5.2.1. Test des modifications du réseau

58. Proximus déclare tester les modifications de manière très approfondie et donne plus d'explications sur la manière dont l'opérateur réalise les tests et rédige le plan de test. Proximus indique également qu'il est impossible de réaliser des tests pour tous les scénarios possibles, mais qu'ils adaptent leur plan de test sur la base de nouveaux incidents qui sont survenus.

59. Proximus a raison, il est impossible de tester tous les scénarios. Actuellement, le nombre de paramètres de matériel et de logiciel est bien trop élevé pour tester toutes les combinaisons dans un laps de temps réaliste. La situation qui s'est produite le 5 avril 2019 consistait en un bug qui est survenu dans des circonstances très spécifiques, dont on peut assumer qu'elles ne sont pas reprises dans un plan de test standard.

5.2.2. Test des systèmes de back-up

60. Proximus déclare tester les modifications de manière très approfondie et donne plus d'explications sur la manière dont l'opérateur réalise les tests et rédige le plan de test. Proximus indique également qu'il est impossible de réaliser des tests pour tous les scénarios possibles, mais qu'ils adaptent leur plan de test sur la base de nouveaux incidents qui sont survenus.

61. Proximus a raison, il est impossible de tester tous les scénarios. Actuellement, le nombre de paramètres de matériel et de logiciel est bien trop élevé pour tester toutes les combinaisons dans un laps de temps réaliste. La situation qui s'est produite le 5 avril 2019 consistait en un bug qui est survenu dans des circonstances très spécifiques, dont on peut assumer qu'elles ne sont pas reprises dans un plan de test standard.

5.2.3. SPOF, diversification et BCP

62. Proximus déclare tester les modifications de manière très approfondie et donne plus d'explications sur la manière dont l'opérateur réalise les tests et rédige le plan de test. Proximus indique également qu'il est impossible de réaliser des tests pour tous les scénarios possibles, mais qu'ils adaptent leur plan de test sur la base de nouveaux incidents qui sont survenus.

63. Proximus a raison, il est impossible de tester tous les scénarios. Actuellement, le nombre de paramètres de matériel et de logiciel est bien trop élevé pour tester toutes les combinaisons dans un laps de temps réaliste. La situation qui s'est produite le 5 avril 2019 consistait en un bug qui est survenu dans des circonstances très spécifiques, dont on peut assumer qu'elles ne sont pas reprises dans un plan de test standard.

64. Proximus donne plus d'explications dans sa réponse concernant les différents aspects et formes de ses BCP. Proximus explique également où se trouvent les SPOF actuellement, à savoir au niveau local (communal). Proximus souligne également la nécessité de disposer d'une bonne expertise au sein de son propre personnel afin de pouvoir résoudre les problèmes en cas d'urgence.

65. Les SPOF au niveau local sont difficiles à exclure, mais cela est possible au niveau central de l'infrastructure critique. Cela doit donc être fait et, là où l'on ne peut pas faire autrement, les mesures doivent être prises pour faire face rapidement et efficacement à une panne d'un SPOF.

66. Ce besoin d'expertise interne est en effet très important.

5.2.4. Planning de migration

67. Proximus explique brièvement comment l'opérateur gère les migrations ainsi que l'implication du fournisseur dans ce cadre. Proximus mentionne également le processus de gestion du changement que l'opérateur utilise ainsi que la disposition en matière de plan de secours qui s'y trouve. Proximus insiste également sur le fait que l'incident du 5 avril 2019 n'a pas été causé principalement par une migration, mais résulte d'une étape de migration qui a eu lieu quelques semaines auparavant. Une fois la cause clairement identifiée, il a été possible de retourner à l'ancienne configuration sans aucun problème.

68. Cette explication correspond aux autres informations que nous avons reçues de la part de Proximus dans le cadre de ce dossier ainsi que d'autres dossiers.

6. Recommandations définitives (juillet 2020)

6.1. Recommandations à court terme

69. Sur la base des éléments précédents du présent rapport, l'IBPT formule quelques recommandations à l'intention de Proximus.

70. Pour mettre en œuvre ces mesures, l'IBPT recommande d'utiliser des normes internationales reconnues, comme les normes issues de la famille ISO27000.

71. À l'automne 2020, l'IBPT vérifiera si ces recommandations sont effectivement suivies. L'IBPT peut prendre ou non à un stade ultérieur une décision sous la forme d'instructions contraignantes, conformément aux articles 114 et 114/2 de la LCE.

6.1.1. Analyse des SPOF et des BCP correspondants

72. Proximus doit réaliser une analyse approfondie des SPOF au sein de son infrastructure critique et des fonctions de réseau critiques. Cette analyse doit être effectuée tant au niveau physique (matériel) que logique (logiciel). Un BCP doit être établi pour chaque SPOF afin de limiter un maximum et le plus rapidement possible l'impact en cas de défaillance. Si une expertise externe est nécessaire pour réparer un SPOF, le BCP doit prévoir une solution afin d'assurer la fonctionnalité du SPOF temporairement, éventuellement à un niveau réduit, si cette expertise externe n'est pas immédiatement disponible en raison de problèmes techniques ou pratiques.

6.1.1.1. Motivation

73. Pour résoudre l'incident du 5 avril 2019, Proximus avait besoin de l'expertise du fournisseur Nokia. Cette expertise provenait en partie des États-Unis.

74. Pour cette intervention, une connexion en bon état de fonctionnement entre le réseau de Proximus et le centre de support de Nokia était donc nécessaire.

75. Le 5 avril 2019, l'incident n'avait eu aucun impact sur la connexion Internet. Toutefois, cela n'est pas à exclure lors d'un futur incident. Il est donc important que les BCP de Proximus tiennent compte de la possibilité que l'expertise externe ne soit pas immédiatement disponible ou accessible.

76. Proximus doit donc prévoir une solution ou procédure de back-up pour pouvoir faire face elle-même dans ce cas à l'impact d'un incident, partiellement ou non.

6.1.2. Traiter les problèmes de l'infrastructure critique avec la plus haute priorité

77. Les problèmes au niveau des composantes de l'infrastructure critique doivent toujours être traités avec le plus haut niveau de priorité. Cela vaut particulièrement lorsque la cause du problème n'est pas claire.

6.1.2.1. Motivation

78. Au cours de la période précédant l'incident, quelques problèmes inexplicables touchaient déjà l'équipement en question.

79. Proximus avait à cet effet ouvert un ticket de support auprès du fournisseur.

80. L'on s'est ensuite rendu compte que le ticket n'avait pas été traité avec la priorité nécessaire.

81. Les tickets concernant les fonctions ou composantes critiques dont la cause sous-jacente n'est pas claire et dont l'impact le plus grave serait très important doivent donc être traités avec un haut niveau de priorité.

6.1.3. Test de l'infrastructure critique et des BCP

82. Proximus doit régulièrement tester les composantes et les fonctions critiques, ainsi que les BCP correspondants, comme imposé par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

6.1.3.1. Motivation

83. En vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, Proximus effectue régulièrement des tests des infrastructures critiques.

84. Ces tests n'ont pas pu éviter un impact important et de longue durée le 5 avril 2019.

85. Il est donc vital que ces tests remplissent les conditions suivantes :

    85.1. Ils doivent être représentatifs d'un problème réel.

    85.2. Il convient non seulement de tester la procédure de réparation technique, mais aussi de tester régulièrement les BCP correspondants en cas de problèmes supplémentaires lors de la réparation.

6.2. Recommandation à long terme

86. L'IBPT recommande fortement à Proximus, tant au niveau physique que logique, de rechercher une diversification des composantes et fonctions critiques de réseau. Il sera ainsi possible d'éviter une panne simultanée de composantes et fonctions entières.

Axel Desmedt
Membre du Conseil

Jack Hamande
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil