Institut belge des services postaux
et des télécommunications

Décision du Conseil de l'IBPT du 9 septembre 2021 concernant la clôture de la procédure d'infraction à l'égard de Proximus pour défaut de garantie d'accès ininterrompu aux services d'urgence

Version non confidentielle

Institut belge des services postaux et des télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 boîte 1 | 1030 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

1. Introduction et procédure

1. Le 12 avril 2021, l'IBPT disposait d'informations concernant Proximus susceptibles d'indiquer une infraction à l'obligation qui lui est imposée en vertu de l'article 107, § 1er/1, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques (« LCE »), de prendre toutes les mesures nécessaires, y compris préventives, pour garantir un accès ininterrompu aux services d'urgence.

2. Sur la base de ces informations et conformément à l'article 21 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (« loi statut de l'IBPT »), l'IBPT a dès lors transmis, le 23 avril 2021, une communication de griefs et de mesures envisagées à Proximus. Conformément à l'article 21 de la loi statut de l'IBPT, Proximus a été invitée à formuler ses remarques par écrit et invitée à une audition le 20 mai 2021.

3. Proximus a pu présenter sa vision des faits lors de l'audition précitée et a soumis ses commentaires écrits à l'IBPT le 25 mai 2021. Proximus considère qu'il n'y a pas d'indication de l'existence d'une infraction et demande de suspendre la procédure d'infraction.

4. Sur la base des informations complémentaires fournies par Proximus, l'IBPT réexaminera la perturbation du réseau des 7 et 8 janvier 2021 ainsi que les actions de Proximus pendant et avant l'incident, conformément à l'article 107, § 1er/1, alinéa 1er, de la LCE.

2. Faits relatifs à la perturbation du réseau des 7 et 8 janvier 2021

5. Les réseaux téléphoniques disposent d'une base de données centrale. Pour le réseau 4G et le réseau VoIP fixe de Proximus, il s'agit du Home Subscriber Server (« HSS »). Chez Proximus, celui-ci se compose de deux parties : un front-end qui est connecté au réseau et sur lequel les messages de signalisation arrivent du réseau, et un back-end sous-jacent (également appelé « OneNDS ») dans lequel sont stockées les données proprement dites des appareils sur le réseau.

6. Ce front-end et ce back-end sont reliés par des connexions sécurisées. Ces connexions sont configurées au moyen d'un nom d'utilisateur « EpsUser » et d'un mot de passe correspondant. Proximus a choisi de créer son propre mot de passe à cet effet et n'utilise donc pas le mot de passe standard de Nokia.

7. [Confidentiel]

8. Le 26 novembre 2020, Nokia a apporté quelques modifications prévues aux back-ends. Toutefois, en raison d'un bug logiciel lors de ces modifications du réseau, le mot de passe de l'« EpsUser » dans toutes les copies du back-end a été réinitialisé par inadvertance au mot de passe standard de Nokia. Et ce, alors que le mot de passe de l'« EpsUser » dans toutes les copies du front-end est resté le mot de passe choisi par Proximus, de sorte que ces mots de passe ne concordaient plus.

9. Cela signifie qu'aucune nouvelle connexion ne pouvait être établie entre les différentes copies du front-end et les différentes copies du back-end. Toutefois, cette différence de mot de passe n'a pas été remarquée à l'époque, car les connexions alors existantes sont restées intactes.

10. Le 3 décembre 2020, cette question du mot de passe a été abordée lors d'une réunion entre Nokia et Proximus, qui portait sur l'état d'avancement de leur « vHLR vHSS project ». Cette discussion a été notée dans le procès-verbal de cette réunion[1], qui a ensuite été transmis à l'ensemble de l'équipe du projet « vHLR vHSS project » par e-mail. Plusieurs ingénieurs, dont certains de Proximus, travaillent dans cette équipe de projet[2].

11. Dans la nuit du 7 au 8 janvier 2021, lors de l'installation planifiée par Proximus d'un correctif logiciel de Nokia, une des copies du back-end a été retirée du réseau téléphonique de Proximus. En conséquence, les connexions entre cette copie du back-end et les différentes copies du front-end ont été interrompues. Les différentes copies du front-end ont essayé de compenser cette connexion interrompue en établissant des connexions supplémentaires avec les autres copies du back-end, mais ces connexions supplémentaires ont échoué en raison de la différence de mot de passe.

12. Chaque front-end dispose d'une sécurité intégrée qui l'empêche de continuer à recevoir du réseau des requêtes auxquelles il ne peut pas répondre. Ainsi, lorsqu'une partie importante

[1] Dans ce procès-verbal, un problème a été signalé avec la description « LDAP password NOK on OneNDS » et le commentaire « PROD OneNDS EpsUser password NOK ? »
[2] Le courrier a ainsi été envoyé à 2 Solution Engineers et 1 Project Engineer de Proximus. Quelques autres ont été mis en copie, à savoir le Team Leader, 2 Project Managers et 1 Engineer de Proximus.

des connexions aux différentes copies du back-end échoue, chaque front-end informe le reste du réseau qu'il ne peut plus répondre aux requêtes. En raison de l'activation automatique de ce mécanisme de sécurité, le réseau 4G et VoIP de Proximus ne disposait plus d'un HSS fonctionnel.

13. En conséquence, le réseau 4G et le réseau VoIP fixe de Proximus ont été indisponibles pendant environ 6 heures. Étant donné que toutes les centrales belges 101 et les centrales 100 et 112 de Bruxelles, du Brabant flamand, de Namur, du Brabant wallon, de la Flandre orientale et de la Flandre occidentale sont connectées au réseau VoIP de Proximus[3], ces centrales d'urgence ont été injoignables pendant ces 6 heures.

14. Proximus dispose d'un Disaster Recovery System (« DRS ») pour ASTRID qui permet, en cas de défaillance de la méthode normalement utilisée, d'acheminer les appels vers les centrales d'urgence précitées via d'autres lignes téléphoniques. Cela implique l'utilisation de lignes téléphoniques spécifiques par centrale d'urgence, au lieu des « business trunks » que Proximus utilise en temps normal. Cependant, ces lignes téléphoniques spécifiques utilisent également le réseau VoIP de Proximus et cette solution d'urgence n'a donc pas fonctionné non plus.

15. Après que Proximus, sur les conseils de Nokia, a modifié les mots de passe dans les différentes copies du back-end pour revenir au mot de passe initialement choisi par Proximus, la situation s'est rétablie. Les connexions entre les différentes copies du front-end et les différentes copies du back-end ont pu être rétablies et, par conséquent, les différentes copies du front-end ont pu à nouveau répondre aux requêtes du réseau environ 6 heures après le début des problèmes.

16. Les autres opérateurs n'ont pas été directement impactés par l'incident. Néanmoins, il y a eu un effet indirect évident : une dégradation importante sur les interconnexions due à l'échec des appels vers les numéros touchés par la panne, dont la majorité des numéros d'urgence.

[3] Toutes ces centrales d'urgence sont gérées par ASTRID, un opérateur de télécommunications spécialisé pour les services de secours et de sécurité en Belgique. ASTRID et Proximus ont conclu un accord commercial pour raccorder toutes les centrales d'urgence au réseau VoIP de Proximus.

3. Analyse

3.1. Cadre de la charge de la preuve

17. L'article 107, § 1er/1, alinéa 1er, de la LCE prévoit ce qui suit :

« Les entreprises fournissant des services téléphoniques accessibles au public prennent, le cas échéant en coordination avec les entreprises qui fournissent les réseaux publics de communications électroniques sous-jacents, toutes les mesures nécessaires, y compris préventives, pour garantir un accès ininterrompu aux services d'urgence. »

18. Ce qui précède concerne une obligation de parvenir à un certain résultat, à savoir un accès ininterrompu aux services d'urgence. Si le résultat visé n'est pas atteint, il appartient à la personne soumise à l'obligation de prouver qu'elle a néanmoins pris toutes les mesures nécessaires pour atteindre ce résultat.

19. Le simple fait que l'accès aux services d'urgence ait été interrompu pendant environ 6 heures à la suite de l'incident chez Proximus permet d'affirmer que Proximus n'a pas atteint le résultat visé par l'article 107, §1er/1, alinéa 1er, de la LCE. C'est à Proximus de prouver que, bien qu'elle n'ait manifestement pas réussi à garantir un accès ininterrompu aux services d'urgence, elle a pris toutes les mesures préventives nécessaires pour y parvenir.

20. Proximus sous-traite une partie de ses activités d'opérateur à Nokia[4]. Bien qu'il s'agisse d'une pratique courante chez les opérateurs, cela ne signifie pas que Proximus n'est plus responsable du respect de ses obligations d'opérateur conformément au cadre réglementaire. C'est Proximus elle-même qui doit prendre toutes les mesures nécessaires, y compris les mesures préventives, pour garantir un accès ininterrompu aux services d'urgence.

21. Cela signifie également que Proximus doit établir des canaux de communication suffisamment étendus et transparents avec ses sous-traitants. La décision de sous-traiter certaines tâches ne peut pas entraîner que des bugs logiciels ou d'autres erreurs se nichent inaperçus dans son réseau, surtout s'ils peuvent engendrer une paralysie du réseau de Proximus. Il est et reste de la responsabilité de Proximus de détecter les erreurs éventuelles en temps utile, ou d'obliger ses sous-traitants à détecter les éventuelles erreurs avec le plus grand soin et à les signaler clairement (et éventuellement à les résoudre eux-mêmes). Dans tous les cas, un haut degré de transparence et une coopération efficace doivent être assurés entre les parties qui se confient mutuellement des tâches aussi critiques.

3.2. Analyse

3.2.1. Généralités

22. Sur la base des informations disponibles à ce moment-là, l'IBPT avait supposé qu'il devait être clair pour Proximus (ou au moins pour Nokia) que la différence de mot de passe observée début décembre 2020 dans la connexion entre le One-DNS (back-end) et le vHSS (front-end virtuel) s'était également propagée à la connexion entre le One-DNS et le HSS

[4] [Confidentiel]

(front-end en service) dans l'environnement de production. Cependant, sur la base des nouvelles informations fournies par Proximus, il semble probable que la différence semblait se limiter pour Proximus et Nokia à la connexion entre le One-DNS et le vHSS[5]. En effet, la différence de mot de passe a été introduite par un patch destiné spécifiquement à l'environnement vHSS. C'est également dans cet environnement uniquement que le problème a été constaté, puisque les connexions LDAP ne fonctionnaient plus et le vHSS ne fonctionnait donc plus.

23. Ainsi, s'il était clair qu'un problème existait dans l'environnement virtuel, Proximus et Nokia ne pouvaient raisonnablement pas supposer que cette anomalie s'était propagée plus loin dans les autres composants redondants et qu'un problème similaire existerait dans l'environnement de production. Dans l'environnement de production, tout avait d'ailleurs continué à fonctionner sans problème.

24. Le fait que ni Proximus ni Nokia n'aient eu le réflexe de vérifier si un problème similaire s'était produit dans l'environnement de production n'indique pas nécessairement une violation de l'obligation de Proximus de prendre toutes les mesures nécessaires conformément à l'article 107, § 1er/1, alinéa 1er, de la LCE. Dans un grand environnement informatique, il est pratiquement impossible de tenir toutes les différentes équipes informées des problèmes survenant dans une autre équipe (d'autant plus lorsque les équipes travaillent séparément sur des systèmes dont l'un est dans un environnement de production et l'autre dans un environnement de laboratoire) et de vérifier si ceux-ci peuvent avoir un impact sur leur propre environnement.

25. L'équipe du projet vHSS avait déjà restauré les connexions LDAP dans l'environnement vHSS à la mi-décembre. Nokia avait alors indiqué qu'elle enquêterait plus avant sur la manière dont la différence de mot de passe avait pu se produire. Cette enquête devait apporter des éclaircissements avant que le vHSS ne soit réellement mis en service, mais Nokia avait encore largement le temps pour cela. En prévision de cette enquête plus approfondie, Nokia avait également explicitement conseillé à Proximus de ne pas simplement corriger la différence de mot de passe sans en comprendre la cause réelle, par crainte d'éventuelles conséquences néfastes imprévues.

26. Comme mentionné, le reste du réseau de Proximus a continué à fonctionner sans problème. Ainsi, rien n'indique que l'équipe du projet vHSS aurait dû savoir ou s'attendre à ce que l'impact de la différence de mot de passe soit plus important que prévu. Le fait que la différence soit passée inaperçue dans le reste du réseau semble plausible. L'affirmation de Proximus selon laquelle le problème semblait pour elle limité à l'environnement vHSS jusqu'à l'incident des 7 et 8 janvier est une affirmation crédible et raisonnable.

27. De plus, l'équipe qui a installé le « Trigger Patch » les 7 et 8 janvier n'avait aucune raison de croire qu'il pouvait y avoir une quelconque différence de mot de passe. En effet, le patch lui-même n'a pas affecté le mot de passe du One-DNS pour le HSS et le mot de passe du HSS pour le One-DNS, et donc un contrôle de cohérence entre ces mots de passe n'était (logiquement) pas prévu non plus dans les vérifications préalables de ce patch.

[5] Il s'agit d'une différence importante, étant donné qu'aucun trafic client n'était encore exécuté sur le vHSS. En effectuant d'abord certains tests dans un environnement virtuel, on évite normalement le risque d'incidents ayant un impact concret sur les utilisateurs finals.

28. En outre, le « Trigger Patch » avait déjà été installé dans l'environnement de laboratoire sans aucun problème au début de 2020, mais à cette époque, le « root-cause-patch » n'avait pas encore été installé dans l'environnement de laboratoire, de sorte que la différence de mot de passe n'y était pas présente. Il n'y avait donc aucune indication que le « Trigger Patch » pouvait causer un problème.

3.2.2. Toutes les mesures préventives nécessaires

29. L'évaluation ci-dessus montre que l'incident n'est pas dû à une quelconque faute ou négligence de la part de Proximus. Toutefois, l'article 107, § 1er/1, alinéa 1er, de la LCE impose une obligation plus étendue à Proximus. En plus d'analyser si l'incident est dû à une faute ou à une négligence de la part de Proximus, il faut également se demander si Proximus a pris toutes les mesures nécessaires, y compris les mesures préventives, pour garantir un accès ininterrompu aux services d'urgence.

30. Comme l'IBPT n'a pas une vue parfaite des éléments techniques et opérationnels du réseau de Proximus, ni de la relation mutuelle entre Proximus et Nokia (y compris les accords opérationnels), il est très difficile pour l'IBPT de vérifier si Proximus a pris toutes les mesures nécessaires, y compris les mesures préventives, pour garantir un accès ininterrompu aux services d'urgence. Il appartient à Proximus d'énumérer toutes les mesures qu'elle a prises à cet égard pour permettre l'évaluation de l'IBPT.

31. Proximus mentionne les considérations pertinentes suivantes :

- Son infrastructure de réseau est basée sur de multiples redondances conçues précisément pour pouvoir contrer les incidents de réseau.
- C'est précisément pour des raisons de sécurité que Proximus utilise ses propres mots de passe sur le réseau. Travailler avec des mots de passe standard est en principe une manière moins sûre de travailler, avec un risque plus élevé d'incidents de réseau et de sécurité.
- L'accès spécifique aux services d'urgence, y compris les redondances prévues à cet effet en termes de lignes de raccordement, a été déterminé en coopération avec ces services d'urgence.
- Les interventions planifiées sur le réseau sont effectuées la nuit, afin de limiter l'impact d'un éventuel incident sur le réseau.
- Les interventions planifiées sur le réseau sont préparées par des tests appropriés en laboratoire, conçus pour éviter les incidents sur le réseau dans la mesure où ils sont raisonnablement prévisibles.
- La différence de mot de passe identifiée dans le HSS virtuel a fait l'objet d'une enquête et d'un suivi. La réinitialisation du mot de passe a été reportée par prudence.
- En parallèle, Proximus a travaillé avec les autorités compétentes et les services d'urgence pour mettre en place une solution d'urgence rapidement opérationnelle et pouvant être communiquée à la population par les canaux appropriés.
- Après l'incident, Proximus, en concertation avec les autorités compétentes et les services d'urgence, a prévu une alternative, similaire à celle mentionnée au point précédent, qui pourrait être activée immédiatement si un tel incident devait se reproduire à l'avenir.

- Proximus déclare avoir toujours soutenu l'initiative visant à garantir l'accès aux services d'urgence via une seconde infrastructure d'un autre opérateur, qui pourrait être activée en cas d'incident sur sa propre infrastructure.

32. Bien que les mesures susmentionnées se soient avérées insuffisantes pour garantir un accès ininterrompu aux services d'urgence, l'IBPT ne peut conclure, sur la base des informations dont il dispose actuellement, que Proximus n'a manifestement pas fait assez pour éviter l'incident en question.

33. L'IBPT prend également acte du fait que Proximus prendra des mesures pour que de tels incidents puissent être traités encore plus rapidement à l'avenir. Il s'agit plus précisément d'une mesure technique supplémentaire permettant de renvoyer les appels d'urgence directement vers les numéros mobiles des services d'urgence. En outre, l'IBPT attend de Proximus qu'elle optimise davantage la redondance du réseau[6] (ou qu'elle prenne d'autres mesures) afin que des incidents similaires n'aient plus le même impact.

34. Dans le même ordre d'idées, suite à cet incident, l'IBPT, en collaboration avec les opérateurs et les services d'urgence, a examiné la possibilité d'une solution redondante via un autre opérateur que Proximus. Étant donné que l'article 107, § 1er/1, alinéa 1er de la LCE impose à Proximus de fournir un accès ininterrompu aux services d'urgence et de prendre toutes les mesures nécessaires à cet effet, l'IBPT attend une coopération totale et proactive de Proximus afin que ce projet puisse contribuer au fonctionnement optimal des services d'urgence. Cela implique également que Proximus alloue les ressources nécessaires pour que cette redondance supplémentaire puisse être réalisée le plus rapidement possible.

35. Compte tenu de l'analyse ci-dessus et des initiatives et mesures citées par Proximus, l'IBPT conclut qu'il n'y a pas d'indication claire d'une infraction au cadre réglementaire, et plus particulièrement de l'article 107, § 1er/1, alinéa 1er, de la LCE. Toutefois, l'IBPT réserve sa position concernant toute information (y compris les communications entre Nokia et Proximus) dont il n'a actuellement pas connaissance.

[6] À cette fin, Proximus a déjà lancé un audit interne pour analyser si et comment la redondance existante sur son réseau peut être renforcée.

4. Consultation des régulateurs médias

36. L'article 3 de l'accord de coopération[7] prévoit la consultation par une autorité de régulation des autres autorités de régulation pour chaque projet de décision relatif aux réseaux de communications électroniques.

37. Les autorités de régulation consultées disposent d'un délai de 14 jours civils pour faire part de leurs remarques à l'autorité de régulation qui a transmis le projet. Dans ce délai, chacune des autorités de régulation consultées peut également demander que la CRC soit saisie du projet de décision. L'autorité de régulation concernée prend en considération les remarques que lui ont fournies les autres autorités de régulation et leur envoie le projet de décision modifié. Ces dernières disposent alors d'un délai de 7 jours civils pour demander que la CRC soit saisie du projet de décision modifié.

38. Un projet de décision a été soumis aux régulateurs des médias le 19 août 2021. VRM, CSA et Medienrat ont indiqué ne pas avoir de commentaires sur le projet de décision.

[7] Accord de coopération du 17 novembre 2006 entre l'État fédéral, la Communauté flamande, la Communauté française et la Communauté germanophone relatif à la consultation mutuelle lors de l'élaboration d'une législation en matière de réseaux de communications électroniques, lors de l'échange d'informations et lors de l'exercice des compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et la télévision, M.B., 28 décembre 2006, 75371.

5. Décision

39. Le 9 septembre 2021, le Conseil de l'IBPT a décidé que, sur la base des informations dont dispose l'IBPT, aucune infraction manifeste ne peut être établie dans le chef de Proximus concernant l'incident de réseau des 7 et 8 janvier 2021. Pour ces raisons, l'IBPT décide de classer sans suite la procédure d'infraction à l'encontre de Proximus.

40. L'IBPT prend cependant acte du fait que Proximus prendra des mesures supplémentaires pour optimiser la redondance et fournir des alternatives performantes en concertation avec les services d'urgence afin de minimiser l'impact de tels incidents. L'IBPT attend également de Proximus qu'elle adopte une attitude constructive et qu'elle contribue activement à la création éventuelle d'une redondance supplémentaire sur le réseau d'un autre opérateur.

6. Voies de recours

41. Conformément à l'article 2, § 1er, de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, vous avez la possibilité d'introduire un recours contre cette décision devant la Cour des marchés, Place Poelaert 1, B-1000 Bruxelles. Les recours sont formés, à peine de nullité prononcée d'office, par requête signée et déposée au greffe de la cour d'appel de Bruxelles dans un délai de soixante jours à partir de la notification de la décision ou à défaut de notification, après la publication de la décision ou à défaut de publication, après la prise de connaissance de la décision.

42. La requête contient, à peine de nullité, les mentions requises par l'article 2, § 2, de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges. Si la requête contient des éléments que vous considérez comme confidentiels, vous devez l'indiquer de manière explicite et déposer, à peine de nullité, une version non confidentielle de celle-ci. L'Institut publie sur son site Internet la requête notifiée par le greffe de la juridiction. Toute partie intéressée peut intervenir à la cause dans les trente jours qui suivent cette publication.

Axel Desmedt
Membre du Conseil

Jack Hamande
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil