INSTITUT BELGE DES SERVICES POSTAUX
ET DES TÉLÉCOMMUNICATIONS

COMMUNICATION DU CONSEIL DE L'IBPT DU 30 AVRIL 2013 CONCERNANT LES RISQUES POTENTIELS D'ATTEINTE À LA SÉCURITÉ DES RÉSEAUX ET SERVICES DE TÉLÉPHONIE MOBILE DANS LE CADRE DES TECHNOLOGIES 2G ET 2.5 G.

Institut belge des services postaux et des télécommunications
Ellipse Building - Bâtiment C - Boulevard du Roi Albert II 35 - 1030 Bruxelles
Tél. 02 226 88 88 Fax 02 226 88 77 http://www.ibpt.be

Sommaire

1. OBJET DE LA COMMUNICATION

Le 17 février 2012, l'IBPT a transmis à Monsieur Johan Vande Lanotte, Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord, un avis concernant les risques potentiels des réseaux et services de téléphonie mobile dans le cadre des technologies 2G et 2.5G (ci-après nommés « réseaux mobiles 2G et 2.5G»). Le 07 juillet 2012, l'IBPT a publié sur son site Internet une version à destination du public de son avis transmis au Ministre.

Conformément aux conclusions de l'avis susmentionné et au plan opérationnel 2013[1] de l'IBPT, une nouvelle étude a été réalisée sur la sécurité des réseaux mobiles 2G et 2.5G.

Cette étude se base essentiellement sur une enquête, menée auprès des principaux fournisseurs belges de services de téléphonie mobile GSM, GPRS et EDGE, concernant les risques potentiels d'atteinte à la sécurité de leurs réseaux mobiles. Cette enquête examine les mesures actuelles et futures que les opérateurs belges ont prises ou prendront afin de garantir l'intégrité et la confidentialité de leurs services GSM, GPRS et EDGE. Une attention particulière a également été portée à la sécurité des messageries vocales.

Durant le dernier quadrimestre 2012, l'IBPT a ainsi interrogé les principaux fournisseurs de services de téléphonie mobile 2G et 2.5G, en l'occurrence Belgacom, Mobistar et KPN Group Belgium, en leur soumettant un questionnaire relatif à la gestion actuelle et future de la sécurité de leurs réseaux mobiles et aux risques d'atteinte à cette dernière.

2. CADRE JURIDIQUE

Sur base des articles 113, 113/1, 113/2, 114, 114/1 et 114/2 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la LCE), l'IBPT dispose de compétences en matière de qualité et sécurité des réseaux et services publics de communications électroniques.

L'article 114, §1er , de la LCE prévoit ce qui suit :

> *« Les entreprises fournissant des réseaux publics de communications électroniques ou des services de communications électroniques accessibles au public prennent les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants. Des mesures sont notamment prises pour réduire au maximum les conséquences des incidents de sécurité pour les utilisateurs et les réseaux interconnectés. »*

L'article 114/2, §2, de la LCE prévoit entre autres ce qui suit :

> *« Les entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public fournissent à l'Institut à sa demande, toutes les informations nécessaires pour évaluer la sécurité ou l'intégrité, ou les deux, de leurs services et réseaux, y compris les documents relatifs à leur politique de sécurité. […] »*

[1] Fiche « *RE-ER/7/2013/03 : Enquête sur la sécurité des réseaux mobiles*» du plan opérationnel 2013 de l'IBPT, février 2013

En outre, l'article 14, §1er, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, dite loi-statut, charge l'IBPT de contrôler entre autre le respect de la loi de la LCE.

L'enquête susmentionnée a été menée sur base de ces dispositions.

3. PORTÉE LIMITEE DE L'ETUDE AUX TECHNOLOGIES 2G ET 2.5G – EXCLUSION DES TECHNOLOGIES 3G ET ULTÉRIEURES.

La présente étude se limite aux services de téléphonie mobile 2G et 2.5G, dénommés « réseaux mobiles » dans le présent document, et se focalise particulièrement sur la sécurité des communications sur la voie radio, c'est-à-dire entre le terminal de l'usager (un téléphone portable par exemple) et les infrastructures du réseau.

3.1. LES TECHNOLOGIES 2G ET 2.5G

L'innovation essentielle des réseaux GSM, GPRS et EDGE par rapport aux technologies de téléphonie mobile précédentes est leur caractère entièrement numérique. Celui-ci apporte une amélioration indéniable des performances (meilleure exploitation des ressources spectrales et régénération de l'information par exemple) et a naturellement conduit au succès que cette génération de réseaux connaît depuis 1991, soit plus de 20 ans. Lors de l'élaboration de ces normes, la sécurité des communications n'avait néanmoins pas l'importance qui lui est accordée aujourd'hui. L'IBPT constate à cet égard que ces normes se basent sur des mécanismes qui peuvent être remis en cause au regard des progrès technologiques récents.

Le réseau GSM est la seconde technologie de téléphonie mobile, dite « 2G », qui supporte entre autres le transfert de la voix et l'échange de courts messages textuels (SMS) par commutation de circuits. Le réseau GPRS[2] est une technologie dérivée du réseau GSM, qui introduit le transfert de données par commutation de paquets. Elle est généralement qualifiée de technologie « 2.5G ». Enfin, le réseau EDGE[3] est une amélioration des réseaux précédents et permet essentiellement d'atteindre des débits de transferts plus importants.

3.2. LES TECHNOLOGIES 3G ET ULTÉRIEURES

La troisième génération (3G) de technologie de téléphonie mobile et les technologies ultérieures proposent d'atteindre des débits supérieurs ouvrant ainsi la porte à des usages multimédias tels que la transmission de vidéo, la visioconférence ou l'accès à internet haut débit. L'élaboration des normes 3G et de générations ultérieures bénéficient de l'expérience acquise, notamment en matière de sécurité, de sorte que ces nouvelles technologies bénéficient de mécanismes de protection plus matures, plus complexes et plus performants que ceux repris dans le cadre du 2G et du 2,5G.

Par ailleurs, les faits majeurs qui ont marqué l'Europe en matière de sécurité des réseaux mobiles (par exemple le scandale du piratage des messageries vocales par *News International* en juillet 2011 ou les critiques de certains experts sur la sécurité des services de téléphonie mobile

---

2 GPRS : *General Packet Radio Service* – Service de transfert de données en commutation de paquets

3 EDGE : *Enhanced Data Rates for GSM Evolution* - Débit de données enrichi pour l'évolution globale.

2G et 2,5G relatés par la presse en décembre 2011) ne concernent pas les technologies 3G et supérieures.

L'analyse de ces réseaux n'est dès lors pas comprise dans la présente étude.

4. ANALYSE INTERNE

L'analyse interne est la résultante des recherches qui ont été réalisées en vue de l'avis de juillet 2012[4] et qui ont été à nouveau effectuées en tenant compte des dernières publications en la matière. A notre meilleure connaissance, l'état de l'art ne montre aucune évolution majeure en terme de risque d'atteinte. En effet, aucune nouvelle brèche majeure n'a été identifiée et aucun nouvel exploit notable n'a été rapporté depuis le précédent exercice.

Comme relaté dans l'avis susmentionné, les vulnérabilités les plus critiques sont

- l'absence d'authentification mutuelle. Il s'agit d'une vulnérabilité inhérente à l'architecture de sécurité : seul le terminal doit confirmer son identité et n'est donc pas en mesure de vérifier à quel réseau il est réellement connecté.
- une négociation des algorithmes de chiffrement[5] (de type A5 ou GEA respectivement pour les réseaux GSM ou GPRS) alors que l'efficacité de ces derniers aurait diminué au regard des avancées technologiques.

5. ANALYSES DES RÉPONSES DES OPÉRATEURS

Les réponses des opérateurs à l'enquête de l'IBPT étant de nature confidentielle, elles ne peuvent être révélées intégralement dans le présent document.

L'analyse réalisée par l'IBPT se limite volontairement à une évaluation qualitative et globale du risque d'atteinte à la sécurité et n'a pas procédé à une analyse quantitative (par exemple le nombre d'usagers affectés). L'IBPT ne peut dès lors quantifier de façon précise le risque d'atteinte à la sécurité.

L'analyse montre néanmoins que les opérateurs témoignent d'une attention particulière envers la sécurité de leur réseau mobile en termes de gestion, d'investissements et de veille technologique. Durant l'année 2012, les opérateurs ont fait évoluer la sécurité de leurs réseaux mobiles et continuent, à l'heure actuelle, d'étudier et de planifier de nouvelles mesures pour accroître davantage le niveau de sécurité de leurs réseaux mobiles.

Concernant les réseaux 2G, nous constatons en Belgique une utilisation pratiquement exclusive d'un algorithme de chiffrement dont l'efficacité serait susceptible d'être éprouvée au regard des derniers progrès technologiques. Le recours généralisé à un algorithme permettant un plus haut niveau de sécurité est en phase d'étude ou d'évaluation auprès des opérateurs, mais il n'est aujourd'hui pas envisageable principalement pour des raisons de compatibilité : plus d'un tiers du parc actuel des terminaux devraient être certainement remplacés. Une approche pragmatique – qui est d'ailleurs notamment adoptée par les opérateurs mobiles - est de dès lors

[4] Voir Section 5.1 - Avis de l'IBPT à destination du public concernant les risques potentiels des réseaux et services de téléphonie mobile dans le cadre des technologies 2G et 2.5G, juillet 2012

[5] Les algorithmes de chiffrement permettent de protéger les informations véhiculées contre toute interception et tout décodage qui ne sont pas autorisés.

renforcer l'algorithme existant en implémentant certaines fonctionnalités récentes des spécifications GSM.

Concernant les réseaux 2,5G, les opérateurs mobiles font l'hypothèse que – pour certaines transmissions - les données soient sécurisées en amont, par exemple, en se connectant à des sites certifiés en HTTPS. Il faut cependant relativiser par l'utilisation effective de ce mode de transmission et par la faible fraction de volume des données mobiles qui sont échangées sur les réseaux 2,5G : environ 75% du trafic s'effectue en effet sur les réseaux 3G et 3,5G.

Les messageries vocales ont reçu une attention spécifique de la part des trois opérateurs.

Dans le cadre de l'enquête, les opérateurs n'ont communiqué à l'IBPT aucun cas de violation avéré de le la sécurité de leurs réseaux mobiles. De plus, aucun problème pertinent n'a été également rapporté par les utilisateurs.

Malgré ces résultats positifs, l'IBPT est d'avis que certains aspects peuvent encore être encore améliorés et attira l'attention des opérateurs sur ces derniers au travers de suivis bilatéraux.

En tout généralité, il faut évaluer toute hausse du niveau de sécurité et prendre en considération les répercussions engendrées aussi bien auprès des opérateurs (charge sur les systèmes, interopérabilité, investissement, etc.) qu'auprès des utilisateurs finals (expérience-client, tarif, qualité de service, etc.). La compatibilité des terminaux tant en national qu'en roaming est certainement un facteur déterminant à considérer.

6. CONCLUSIONS

Dans le cadre de l'enquête, les opérateurs n'ont communiqué à l'IBPT aucun élément tangible ou soupçon de violation de la sécurité de leurs réseaux mobiles. Depuis la précédente enquête, les opérateurs ont adopté et planifié de nouvelles mesures pour renforcer la sécurité de leurs réseaux mobiles.

L'analyse des réponses des opérateurs et la confrontation de ces dernières aux standards actuels amène à penser que la sécurité de leurs réseaux mobiles est aujourd'hui satisfaisante mais peut être encore améliorée à différents niveaux.

A cette fin, l'IBPT a le projet de lancer une dynamique d'échanges avec les opérateurs mobiles pour discuter de ces questions d'amélioration et surtout pour dégager des solutions pragmatiques et proportionnelles. L'IBPT veillera également à ce que les mesures de sécurité que les opérateurs mobiles ont planifiées deviennent effectives. Si nécessaire, l'IBPT étudiera la possibilité d'imposer certaines instructions contraignantes conformément à l'article 114/2, §1er, de la LCE.

En tout état de cause, l'IBPT reconsidérera sa position au fil de l'apparition des éléments nouveaux ou suite à toute nouvelle enquête.