Institut belge des services postaux
et des télécommunications

Consultation concernant le projet de communication sur les analyses de risque en matière de sécurité des réseaux et des systèmes d'information

Comment réagir au présent document ?

Jusqu'au 15/09/2020
Uniquement par e-mail à consultation.sg@ibpt.be
Avec la référence CONSULT-2020-D1

Personne de contact : Pierre-Francois Vandenhaute, Ingénieur-conseiller (+32 2 226 89 78)

Les réponses sont attendues uniquement par voie électronique à l'adresse précisée

Merci de joindre ce formulaire de couverture à votre réponse.

Vos commentaires devraient se référer aux paragraphes et/ou sections auxquels ils se rapportent et indiquer clairement ce qui est confidentiel.

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

Partie I. Introduction

1. L'IBPT entend demander aux opérateurs de lui soumettre annuellement une analyse de risque et, sur cette base, d'évaluer les principales composantes des risques au niveau national au profit des autorités publiques et des opérateurs. Pour cela, l'IBPT met à disposition la plateforme SERIMA.be.

2. Le projet de communication soumis à consultation est présenté dans la partie 2.

3. L'IBPT souhaite rassembler toutes observations ou remarques pertinentes concernant ce projet de communication.

Partie II. Projet de communication

1. Objet

4. Le secteur des communications électroniques (en ce compris les infrastructures numériques) comprend des éléments essentiels pour le fonctionnement de la société et des services publiques. La sécurisation de tous les éléments, aussi bien matériels qu'organisationnels, doit être une priorité de tous les acteurs de ce secteur. Les interdépendances multiples entre les différents acteurs et services doivent inciter chaque acteur à atteindre un niveau de sécurité suffisant pour protéger ses propres activités mais également les services d'autres acteurs du secteur.

5. Dans ce contexte, l'article 114, § 1er, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la « LCE ») prévoit que chaque opérateur télécom doit prendre les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services. Compte tenu des possibilités techniques les plus récentes, ces mesures doivent garantir un niveau de sécurité adapté aux risques existants.

6. L'article 20 de la loi NIS[1], qui s'applique aux opérateurs de services essentiels (OSE) entre autres du secteur des infrastructures numériques, comprend une disposition similaire. L'IBPT a été désigné comme autorité sectorielle et service d'inspection pour ce secteur dans le cadre de la loi NIS et a procédé à la désignation des OSE. Les OSE et les opérateurs télécoms sont désignés ci-après les « opérateurs ».

7. La présente communication a pour objectif d'informer le secteur de la mise en place par l'IBPT d'un nouvel outil d'analyse de risques en matière de sécurité des réseaux et systèmes d'information, sous la forme d'une plateforme en ligne (ci-après « la plateforme SERIMA.be »[2]). Cet outil est voué :

   - à faciliter l'échange d'informations entre les opérateurs et l'IBPT, notamment dans le cadre du contrôle du respect de l'article 114, §1er, al. 1er, de la LCE et de l'article 20, § 1er, de la loi NIS, et ;
   - à permettre aux opérateurs de s'auto-évaluer et d'accroître leur niveau de sécurité.

8. Dans un premier temps, l'IBPT demandera aux OSE et à certains opérateurs télécom (vu leur importance significative pour la société et l'économie belges) d'utiliser la plateforme SERIMA.be. Les autres opérateurs télécom peuvent faire usage de l'outil en adressant une demande à l'IBPT et moyennant le respect des conditions visées dans la présente communication. Dans un deuxième temps et sur base d'un retour d'expérience, l'IBPT examinera l'opportunité d'élargir le nombre d'utilisateurs de la plateforme.

9. Du 22/07/2020 au 15/09/2020, le projet de la présente communication a fait l'objet d'une consultation publique.

[1] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
[2] Abréviation de « Security Risk Management ».

2. Cadre juridique

10. En vertu de l'article 8, 6° LCE, il revient à l'IBPT la tâche de veiller à l'intégrité et la sécurité des réseaux publics de communications électroniques et à la sécurité des services publics de communications électroniques.

11. Par ailleurs, conformément à 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 (loi statut), l'IBPT est chargé de contrôler le respect des dispositions de la LCE et de la loi NIS pour ce qui concerne le secteur des infrastructures numériques.

12. L'article 114/2, §1er, de la LCE précise que, dans le cadre de ce contrôle, l'IBPT a le pouvoir de donner des instructions contraignantes, y compris concernant les dates limites de mise en oeuvre, aux opérateurs télécoms.

13. L'IBPT peut également, conformément à l'article 114/2, § 2 LCE, solliciter de ces mêmes opérateurs télécoms 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 (alinéa 1er), ainsi que soumettre ces opérateurs télécoms à un contrôle de sécurité effectué par un organisme qualifié indépendant ou l'Institut lui-même (alinéa 2).

14. Par ailleurs, l'IBPT a été désigné comme service d'inspection pour le secteur des infrastructures numériques dans le cadre de la loi NIS, qui prévoit entre autres que :

- « Les services d'inspection peuvent à tout moment réaliser des contrôles du respect par l'opérateur de services essentiels des mesures de sécurité et des règles de notification des incidents. » (article 42, § 1er) ;
- Le service d'inspection peut formuler une demande d'informations ou de preuves (article 42, § 3) ;
- « L'opérateur de services essentiels apporte son entière collaboration aux membres du service d'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes. » (article 46, § 1er).

3. Mesures de sécurité et analyse de risques

15. L'obligation prévue à l'article 114, § 1er, alinéa 1er, de la LCE, d'adopter des mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services et l'obligation équivalente à l'article 20 de la loi NIS, supposent l'établissement et la mise à jour régulière d'un système de gestion de la sécurité de nature à permettre une analyse des risques adéquate.

16. Une analyse de risques se compose de trois étapes principales [3] :

- L'identification des risques ;
- L'évaluation des risques ;
- La gestion des risques.

17. Pour être performante, une analyse de risque doit répondre aux conditions suivantes :

- être exécutée pour tous les actifs répertoriés d'une entreprise[4] ;
- confronter les actifs avec des menaces ;
- pour chaque couple d'actif-menace, identifier les vulnérabilités ;
- sur la base de l'identification des vulnérabilités, adopter des mesures de sécurité visant à supprimer, ou à défaut de réduire, l'impact et/ou la probabilité de l'exploitation d'une vulnérabilité et, par conséquence, supprimer, ou à défaut réduire, le risque.

[3] Ceci découle des normes en matière de sécurité des réseaux : ISO/IEC 27005, NIST Special Publication 800-37, BS 7799-3 BSI.
[4] Par définition, les actifs d'une société représentent toutes les ressources matérielles, humaines, administratives ou organisationnelles rentrant en compte dans la fourniture de ses services ou produits.

4. La plateforme SERIMA.be

4.1. Description générale

18. La plateforme SERIMA.be permet d'effectuer une analyse complète des risques selon la méthodologie prévue par la norme ISO/IEC 27005 relative aux technologies de l'information, techniques de sécurité et gestion des risques liés à la sécurité de l'information, qui constitue une norme pertinente pour l'application de différentes réglementations incluant des aspects de gestion de risques, comme l'article 114, § 1er, de la LCE, l'article 20 de la loi NIS et le RGPD[5]. L'IBPT n'examinera bien entendu que le respect de la LCE et de la loi NIS (pour le secteur des infrastructures numériques).

19. Compte tenu des contextes multiples d'application de la norme ISO/IEC 27005, la plateforme SERIMA.be a été conçue pour permettre aux entreprises de sélectionner les risques pertinents à soumettre à l'autorité compétente pour une réglementation donnée. Une fois insérée dans la plateforme, ces données pourront être soumises au(x) régulateur(s) pertinents en totalité ou en partie, selon les paramètres sélectionnés par l'entreprise.

20. En outre, la plateforme SERIMA.be peut être utilisée par tout opérateur ayant accès à cette dernière, comme système de gestion des risques pour d'autres référentiels[6], tels que les référentiels propres à l'entreprise.

21. La plateforme SERIMA.be a vocation à évoluer, selon le retour d'expérience (« feedback ») de ses utilisateurs, notamment en ce qui concerne la mise à jour des librairies, la correction des fonctionnalités existantes ainsi que l'ajout d'éventuelles fonctionnalités.

22. La plateforme SERIMA.be permet à tout opérateur télécom de réaliser une analyse de risque appropriée et d'évaluer les mesures de sécurité déjà en place en son sein, selon la méthodologie décrite dans les « Technical guidelines of security measures »[7] de l'ENISA. Les éléments pertinents pour l'IBPT, dans le cadre de ses missions légales, peuvent ensuite être sélectionnés par l'entreprise et transmis à l'IBPT.

4.2. Objectifs visés

23. La plateforme SERIMA.be a pour objectif premier de faciliter l'échange d'informations entre les opérateurs et l'IBPT dans le cadre du contrôle du respect de la LCE et la loi NIS.

24. Plus précisément, la transmission des informations par le biais de la plateforme SERIMA.be permettra à l'IBPT :

- de disposer d'un aperçu plus clair et précis quant au niveau de sécurité de chaque opérateur en matière de sécurité des réseaux et services ;

[5] Règlement nº 2016/679, dit règlement général sur la protection des données.
[6] ISO27001, GDPR ou un référentiel défini par l'entreprise.
[7] https://resilience.enisa.europa.eu/article-13

- d'observer l'évolution de la situation d'un opérateur d'année en année ;
- de comparer de manière aisée et automatisée les données entre opérateurs, grâce au recours à une même méthodologie et à la standardisation du format des données.

25. En outre, l'observation sous une forme agrégée des données transmises à la plateforme SERIMA.be permettra à l'IBPT d'en tirer les enseignements utiles, tels que par exemple l'identification des risques communs à la plupart ou à l'ensemble des opérateurs, les bonnes pratiques pour ce qui concerne les mesures de sécurité, etc. Ces observations permettront notamment de contribuer à fixer les niveaux de priorité de ses domaines d'intervention.

26. Par ailleurs, l'IBPT pourra faire bénéficier le secteur de ces enseignements :

- Par la transmission à chaque opérateur utilisant la plateforme, après examen des données transmises par le biais de cette plateforme, d'un rapport générique et d'un rapport individuel de leur gestion des risques afin de les soutenir dans leur gestion de la sécurité;
- Par la publication d'un rapport général d'aide à la gestion des risques à destination de tous les acteurs du secteur.

4.3. Informations pratiques

4.3.1. Accès à la plateforme

27. La plateforme de gestion des risques SERIMA.be est accessible à l'adresse suivante : https://serima.be.

28. Les accès doivent être demandés par email à net.sec@bipt.be.

29. Un accès par opérateur est fourni par l'IBPT. Plusieurs utilisateurs d'un même opérateur peuvent utiliser cet accès.

4.3.2. Informations à prendre en compte

30. Pour que l'analyse de risque via SERIMA.be soit efficace, il convient de répondre à un certain nombre d'éléments.

31. Les services suivants sont par défaut à considérer dans l'analyse :

- Fibres (noires) ou réseau de fibres : exploitation, mises à disposition et/ou maintenance de ces fibres ;
- Données : mobile, fixe, transit, interconnexions, VPN ;
- Voix : mobile, fixe, interconnexions ;
- Vidéo (à l'exception de la TV et de la radio) : mobile, fixe, interconnexions ;
- Messagerie: messagerie instantanée, SMS, email.

32. Tant les services de communications électroniques de détail (« retail ») que les services aux entreprises (« business ») et à d'autres opérateurs (« wholesale ») sont à considérer lors de l'utilisation de la plateforme, puisque chacun de ces types de services est susceptible d'avoir un impact significatif sur le bon fonctionnement de la société et de l'économie.

33. Pour qu'une soumission soit valide, les informations marquées « obligatoires » dans la plateforme SERIMA.be doivent avoir été remplies avec exactitude et probité. Il s'agit :

- des données générales du projet ;
- des données définissant le contexte de l'analyse de risque ;
- des données liées à l'analyse de risque pour l'ensemble des service offerts, des actifs qui les supportent, à mettre en relation avec au minimum les menaces reprises comme « obligatoires » ;
- des données décrivant les mesures déjà en place et l'évaluation du niveau de sécurité.

34. Pour les années 2021 et suivantes, les opérateurs sont invités à soumettre ce formulaire à l'IBPT au minimum une fois par an, entre le 1 avril et le 30 juin au plus tard, par le biais de la plateforme SERIMA.be mise à leur disposition ou en fournissant à l'IBPT un export de leur propre plateforme SERIMA.be.

35. Dans le cas où l'IBPT rejette de manière motivée la soumission du formulaire au motif que cette dernière n'est pas valide, l'opérateur a la possibilité de soumettre un formulaire corrigé dans le délai fixé par l'IBPT.

4.3.3. Formations

36. Des formations à l'utilisation de la plateforme SERIMA.be seront proposées périodiquement par l'intermédiaire de l'IBPT.

37. Des tutoriels sous forme de vidéos seront également disponibles.

5. Conclusions

38. Dans un premier temps, l'IBPT demandera aux OSE et à certains opérateurs télécom (vu leur importance significative pour la société et l'économie belges) d'utiliser la plateforme SERIMA.be. Les autres opérateurs télécom peuvent faire usage de l'outil en adressant une demande à l'IBPT et moyennant le respect des conditions visées dans la présente communication. Dans un deuxième temps et sur base d'un retour d'expérience, l'IBPT examinera l'opportunité d'élargir le nombre d'utilisateurs de la plateforme.

39. Après examen des données transmises par le biais de la plateforme SERIMA.be, l'IBPT transmettra à chaque opérateur un rapport générique et un rapport individuel de leur gestion des risques afin de les soutenir dans leur gestion de la sécurité.

Axel Desmedt
Membre du Conseil

Jack Hamande
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil