Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de télécom CRTC 2018-62

Version PDF

Ottawa, le 15 février 2018

Dossier public : 8621-C12-01/08

Groupe de travail Plan de travail du CDCI – Rapport de consensus BPRE096a concernant l'état de préparation des entreprises canadiennes relativement à la mise en œuvre du protocole Transport Layer Security par l'intermédiaire du protocole Applicability Statement 2

Contexte

1. En 2015 et 2016, le Groupe de travail Plan de travail (GTPT) du Comité directeur du CRTC sur l'interconnexion (CDCI) a déployé des efforts pour améliorer la sécurité du protocole Applicability Statement 2 (AS2), un protocole électronique de transfert de fichiers utilisé par les fournisseurs de services de télécommunication (FST) exerçant des activités au Canada pour échanger des données[1] sur Internet. Le projet a permis de cerner certains éléments de la cryptographie du transfert de fichiers actuellement utilisés et de définir une marche à suivre pour améliorer la sécurité des certificats numériques[2] utilisés dans le protocole AS2.
2. Grâce à ces efforts, le GTPT a présenté une série de rapports qui ont été approuvés par le Conseil dans différentes décisions[3]. Dans ces décisions, le Conseil a approuvé les recommandations du GTPT, qui ont donné lieu à la création d'une nouvelle version mise à jour des Lignes directrices canadiennes relatives à l'échange de données, où figurent les lignes directrices de l'industrie concernant l'échange électronique de fichiers de données d'affaires entre les FST.
3. Toutefois, pendant le déploiement des améliorations de la sécurité de l'échange de fichiers, certains problèmes de compatibilité entre les protocoles AS2 des FST ont été signalés. Ces problèmes étaient dus à l'utilisation de méthodes différentes pour la mise en œuvre des suites de chiffrement[4] dans la version normalisée 1.2 du protocole Transport Layer Security (TLS)[5].

---

[1] Ces données incluent des renseignements sur les commandes de service local, les inscriptions à l'annuaire, les demandes et les données de services interurbains, et des données sur la facturation et les recouvrements.

[2] Les certificats numériques sont des justificatifs d'identité électronique qui sont utilisés pour certifier l'identité électronique des individus, des organisations et des ordinateurs. Ils sont émis et certifiés par une autorité de certification comme Entrust.

[3] Voir les décisions de télécom 2015-435, 2016-150 et 2017-31.

[4] Une suite de chiffrement est une combinaison d'algorithmes d'authentification et de cryptage utilisés pour franchir les paramètres de sécurité et se connecter à un réseau qui utilise des protocoles de réseau Secure Sockets Layer (SSL) et Transport Layer Security (TLS).

[5] La couche transport du protocole AS2 comprend un protocole de transfert hypertexte (HTTP) et un protocole SSL ou TSL aux fins de sécurité. Ce protocole est appelé « protocole HTTPS ». Le

4. Afin de résoudre les problèmes de compatibilité, le GTPT a recommandé une modification des Lignes directrices canadiennes relatives à l'échange de données afin d'exiger que les FST utilisent la suite de chiffrement dont la « mise en œuvre est obligatoire » contenue dans la version normalisée 1.2 du protocole TLS de l'Internet Engineering Task Force (IETF), modification que le Conseil a approuvé dans la décision de télécom 2017-31.

5. Les membres du GTPT ont également convenu de continuer de saisir des occasions d'améliorer la sécurité de la cryptographie tout en continuant d'utiliser la version 1.2 du protocole TLS. Le GTPT a précisé que même si la version normalisée 1.3 du protocole TLS était encore en cours d'élaboration, il semblait y avoir consensus dans cette version à l'égard de l'élément de la suite de chiffrement dont la mise en œuvre est obligatoire. Par conséquent, le GTPT a étudié les options de mise en œuvre de la version 1.3 provisoire du protocole TLS. Le GTPT a également convenu que la normalisation d'une suite de chiffrement dont la mise en œuvre est obligatoire lui permettrait d'adapter ses activités aux besoins futurs si une mise à niveau à la version 1.3 du protocole TLS était effectuée.

Le rapport

6. Le 16 octobre 2017, le Conseil a reçu du GTPT un rapport intitulé *Readiness of Canadian Carriers to Implement Enhanced Transport Layer Security via AS2* (BPRE096a, *État de préparation des entreprises canadiennes relativement à la mise en œuvre du protocole Transport Security Layer par l'intermédiaire du protocole Applicability Statement 2*) [le rapport][6]. Dans ce rapport, le GTPT faisait le point sur les problèmes liés à la sécurité de l'échange de fichiers dans le protocole AS2 avec la version 1.3 du protocole TLS.

7. Le GTPT a déclaré que la majorité de ses membres ne prenaient pas en charge la suite de chiffrement dont la mise en œuvre est obligatoire identifiée dans la version 1.3 du protocole TLS et qu'ils n'avaient aucun plan ni date officiel concernant sa prise en charge par leurs fournisseurs existants de protocole AS2.

8. Le GTPT a fait remarquer qu'un examen de la version 1.3 du protocole TLS a révélé que la structure de la suite de chiffrement de la version 1.3 du protocole TLS était différente de celle de la suite de chiffrement de la version 1.2 du protocole TLS. Il a conclu qu'il serait impossible d'adopter une approche adaptée aux besoins futurs utilisant les suites de chiffrement dont la mise en œuvre est obligatoire contenues dans la version 1.3 du protocole TLS.

---

protocole TLS est plus récent que le protocole SSL. Dans la décision de télécom 2016-150, le Conseil a approuvé l'utilisation de la version 1.2 du protocole TLS au lieu du protocole SSL.

[6] Le rapport peut être consulté sous la rubrique « Rapports » de la page du GTPT, dans la section du CDCI sur le site Web du Conseil à l'adresse www.crtc.gc.ca.

9. Le GTPT a indiqué que le processus de normalisation de la version 1.3 du protocole TLS entamé par l'IETF prendra bientôt fin. Il a déclaré que plusieurs fournisseurs de logiciels ouverts affirment déjà qu'ils prennent en charge la version 1.3 du protocole TLS et que certains navigateurs Internet populaires comme Google Chrome et Mozilla Firefox prennent en charge la version 1.3 du protocole TLS dans leur mode d'essai et de développement.

10. Le GTPT a conclu que la version 1.3 du protocole TLS devrait être normalisée et largement utilisée d'ici un à trois ans et que cet échéancier est conforme à l'échéancier d'un à trois ans de la plupart des entreprises en ce qui concerne la planification et l'établissement du budget des technologies de l'information avant la mise en œuvre. Le GTPT a donc décidé d'adopter une approche proactive en rappelant aux entreprises qu'elles devront un jour se conformer en mettant en place la version 1.3 du protocole TLS.

11. Par conséquent, le GTPT a demandé au Conseil d'approuver le rapport et d'informer les FST canadiens :

    - des plans de l'industrie des télécommunications relativement à la mise en œuvre de la version 1.3 du protocole TLS (après que l'IETF l'ait approuvée comme une norme) en tant que composante obligatoire du processus relatif au protocole AS2 dans les Lignes directrices canadiennes relatives à l'échange de données;

    - de la nécessité de planifier et de budgétiser les dépenses connexes au titre des logiciels.

Résultats de l'analyse du Conseil

12. Dans la décision de télécom 2015-435, le Conseil a approuvé une mise à jour des exigences relatives à l'échange de données entre les FST ainsi qu'un calendrier de transition mis à jour s'échelonnant sur un an. Dans ce cas, les membres du GTPT ont cessé d'utiliser une norme qui avait été publiée en 1993 pour utiliser une norme qui a été publiée pour la première fois en 2001. Dans la décision de télécom 2016-150, le Conseil a approuvé d'autres améliorations de la sécurité qui comprenaient la transition à la version 1.2 du protocole TLS qui avait été émise en 2008. Le Conseil estime qu'il est raisonnable de présumer que la mise en œuvre de la version 1.3 du protocole TLS prendra également plusieurs années.

13. L'approche proactive adoptée par le GTPT pour examiner les améliorations de la sécurité à venir est louable et est dans l'intérêt des consommateurs, dont les renseignements seront mieux protégés. Le Conseil estime qu'après l'approbation du rapport et le rappel aux entreprises pour les informer que la version 1.3 du protocole TLS sera éventuellement intégrée aux Lignes directrices canadiennes relatives à l'échange de données, i) les entreprises tiendront compte du fait qu'elles pourraient devoir assumer des coûts de transition qu'elles devront inclure dans leur budget et ii) les FST pourraient adopter la version 1.3 du protocole TLS plus tôt que prévu.

14. Par conséquent, le Conseil **approuve** le rapport. Le Conseil avise par la présente les entreprises de se préparer à mettre en œuvre les améliorations de la sécurité à venir prévues dans la version 1.3 du protocole TLS et de prévoir un budget pour leur mise en œuvre.

Secrétaire général

Documents connexes

- *Groupe de travail Plan de travail du CDCI – Rapport de consensus BPRE093c concernant des lignes directrices canadiennes modifiées relatives à l'échange de données*, Décision de télécom CRTC 2017-31, 2 février 2017

- *Groupe de travail Plan de travail du CDCI – Rapport de consensus BPRE093b concernant des lignes directrices modifiées canadiennes relatives à l'échange de données*, Décision de télécom CRTC 2016-150, 26 avril 2016

- *Groupe de travail Plan de travail du CDCI – Calendrier de transition concernant l'échange sécurisé de fichiers de données entre les fournisseurs de services de télécommunication et les fournisseurs de logiciels (rapport BPRE093a)*, Décision de télécom CRTC 2015-435, 23 septembre 2015