Norme minimale TIC : outil d'évaluation : l'instrument d'une protection des données efficace?

Autor(en): **Ferreira, David**

Objekttyp: **Article**

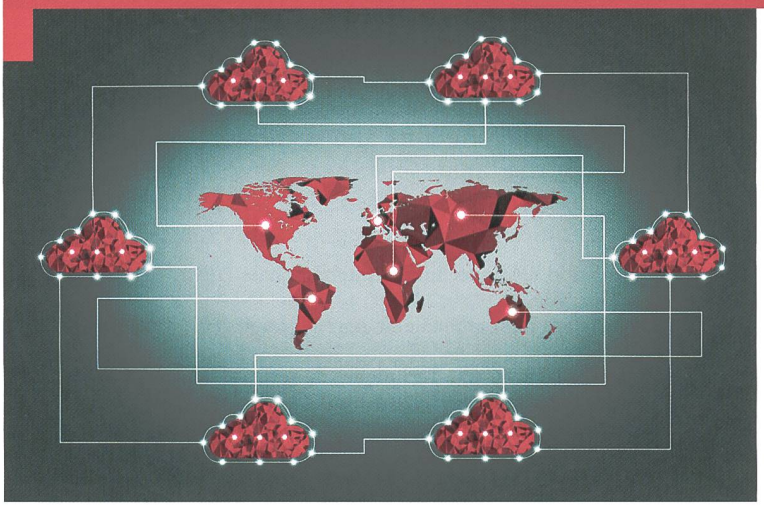
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2019)**

Heft 1

PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-867926



Cyber

Norme minimale TIC - outil d'évaluation : L'instrument d'une protection des données efficace ?

David Ferreira
Data protection officer, ICON 2018

Le Conseil fédéral, conscient des vulnérabilités liées aux cyberrisques, se doit de protéger les infrastructures critiques de notre pays. Dans l'optique de prévenir ces risques, il a adopté, le 18 avril 2018, la nouvelle Stratégie Nationale de Protection de la Suisse contre les Cyberrisques (ci-après : SNPC), pour les années 2018 à 2022, qui cible principalement les infrastructures critiques gérées pour une grande partie par des entreprises privées. [1]

Parallèlement à cette nouvelle mouture de la SNPC, la Confédération a créé une Norme minimale pour les TIC – outil d'évaluation. Cet instrument fixe la norme minimale souhaitée pour les Technologies de l'Information et de la Communication (ci-après : TIC) et invite les exploitants d'infrastructures critiques à la mettre en œuvre. Cet outil *« s'adresse aussi aux entreprises ou organisations intéressées qui recevront ainsi une aide bienvenue pour améliorer la résilience de leurs TIC »*.[2]

Cet article se propose d'étudier, selon quatre approches différentes, les « tâches » sélectionnées par cet outil d'évaluation afin de déterminer s'il est réellement suffisant pour prévenir des cyberrisques dans une infrastructure critique.

Contexte politique :[3]

Ce n'est pas nouveau que la protection des infrastructures critiques soit au centre des préoccupations du Conseil fédéral. Toutefois, ce n'est qu'en 2012 qu'il a approuvé une première stratégie nationale (PIC), avant de l'actualiser en 2017. Cette nouvelle version définit, pour les années 2018 à 2022, les objectifs et les principes pour la protection des infrastructures critiques. Ces objectifs se déclinent en dix-sept mesures rédigées en vue d'améliorer la résilience de la Suisse. Il revient aux autorités responsables de vérifier, dans tous les secteurs, s'il existe des risques notables et, au besoin, de convenir d'une liste de mesures permettant de renforcer la sécurité. Cette liste sera actualisée périodiquement pour les points d'importance. L'un d'eux touche aux TIC. D'ailleurs, il est tellement important que le Conseil fédéral a fait établir la SNPC construite sur le même modèle que la PIC.

L'outil d'évaluation n'aborde pas les enjeux politiques, bien qu'il traite de gouvernance pour les infrastructures critiques. Néanmoins, il en ressort clairement une concrétisation de la PIC, puis de la SNPC, démontrant la volonté politique de préserver des cyberrisques nos infrastructures critiques.

Approche légale :

La Loi sur la Protection des Données (ci-après : LDP; RS 235.1) fait référence en la matière. Cette loi a pour objectif de « protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données » (art. 1) et se divise en deux parties : l'une concerne le secteur privé (art. 13 al. 2 let. e) et l'autre s'applique aux organes fédéraux (art. 22). Les installations critiques relevant du secteur public, regardons les exigences de la seconde partie, soit notamment l'anonymisation et la sécurisation des données, leur conservation ou l'explication du but de leurs traitements.

L'outil d'évaluation rappelle que les infrastructures critiques doivent obéir aux conditions de la Loi fédérale sur l'approvisionnement économique du pays (Loi sur l'approvisionnement du pays, LAP ; RS 531), l'Ordonnance sur l'approvisionnement économique du pays (OAEP ; RS 531.11) et l'Ordonnance sur les préparatifs en matière d'approvisionnement économique du pays (RS 531.12) qui n'est cependant plus en vigueur depuis le 1er juin 2017. Toutefois, il ne mentionne pas la LPD, même si différents critères, tels que le cryptage de données ou encore le niveau de sécurité appliqué par les sous-traitants, sont des exigences propres à la LPD.

Par conséquent, l'outil d'évaluation couvre parfaitement la sécurisation des données, leur anonymisation ou encore la vérification des normes à toutes les échelles, y compris chez les sous-traitants. La comparaison s'arrête là ! En effet, certaines obligations découlant de la LPD, par exemple la réutilisation ou le temps de conservation des données, ne sont pas présentes dans l'outil. Par conséquent, l'outil a été pensé et créé autour de la sécurisation des données, mais il n'a pas pris en compte intégralement la LPD.

Du point de vue technique:

Référence est faite au Guide relatif aux mesures techniques et organisationnelles de la protection des données.[4] Rédigé par le Préposé fédéral à la Protection des Données et de la Transparence et paru en août 2015, il a pour but d'aider à mettre en œuvre une protection optimale des données. Il se divise en quatre thématiques : l'accès aux données, le cycle des données, le transfert des données et l'accès aux données.

L'outil d'évaluation reprend des mesures clés de différentes documentations et normes: NIST Guide to Industrial Control Systems, ISO 2700x, Cobit, ENISA Good Practice Guide on National Cyber Security Strategies et Bundesamt für Sicherheit in der Informationstechik. Ce choix permet à l'outil d'être très complet et couvre les exigences du Guide relatif aux mesures techniques et organisationnelles de la protection des données. Même l'accès aux données y apparaît puisque la partie gouvernance prévoit son organisation.

En somme, l'outil d'évaluation suffit à couvrir techniquement les infrastructures critiques en matière de protection des données.

L'aspect financier :[5]

En cybersécurité, il est très difficile de lister les éléments financiers. En effet, l'investissement n'a pas de réel retour et les fonds investis pour la cybersécurité sont généralement inclus dans un budget plus large. La question est donc: comment établir un budget? Une des méthodes consiste à faire une estimation des pertes financières selon les risques et de combler les risques les plus importants. Le rapport « Evaluation d'approches coûts-utilité », élaboré à Davos en 2013, peut être utilisé comme référence pour nos infrastructures critiques. Des calculs effectués sur la base de scénarios catastrophes mettent en évidence les risques les plus importants et en donnent une estimation chiffrée. A partir de ce document, les entreprises exploitantes des infrastructures critiques sont invitées à établir un budget incluant les risques à couvrir.

L'outil d'évaluation n'aborde pas directement l'aspect financier. Néanmoins, si l'outil est bien exécuté, il permettra d'atténuer, voire d'éviter les conséquences des scénarios catastrophes, comme les cas cités dans le rapport de Davos, et de faire donc des économies.

Synthèse:

Pour conclure, nous avons cherché à savoir si le nouvel outil d'évaluation de la Confédération est suffisant pour prévenir des cyberrisques dans une infrastructure critique. Pour cela, nous l'avons examiné sous différentes approches: malgré que les tâches considérées par l'outil d'évaluation soient peu diversifiées, la plus grande partie des exigences en matière de protection des données sont couvertes. Les lacunes relevées (réutilisation ou encore temps de conservation des données) démontrent que l'outil d'évaluation ne considère que la mise en œuvre et les aspects techniques de la protection des données au détriment d'une vision globale.

Cette petite faiblesse est à relativiser au regard de la volonté manifeste des autorités politiques suisses de renforcer le domaine de la protection des données. De plus, cette proactivité permettra à coup sûr de faire des économies en cas de crise. L'outil d'évaluation s'insère ainsi parfaitement parmi les mesures déjà en place et s'avérera pour sûr très utile.

D. F.

1. P.15 SNPC 2018.
2. https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html .
3. https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html
4. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html
5. https://www.babs.admin.ch/fr/aufgabenbabs/ski/publikationen.html#ui-collapse-764