26 août 2021, 22h28 **21.176**

Interpellation du groupe socialiste

Quelles mesures pour garantir la sécurité informatique des collectivités publiques neuchâteloises ?

La commune de Rolle (VD) a récemment été victime d'un piratage massif de données personnelles concernant ses habitant-e-s. Ces données comprennent notamment des numéros de téléphone, des numéros AVS et des informations sur l'appartenance religieuse. Des documents confidentiels au niveau politique et stratégique ont également été rendus publics, ainsi que des informations détaillées sur les employé-e-s de la commune. Il est à relever que ce piratage s'inscrit dans une recrudescence des attaques envers les administrations publiques observée de manière plus générale.

À Neuchâtel, c'est le service informatique de l'entité neuchâteloise (SIEN) qui est en charge de l'infrastructure informatique de la plupart des entités publiques et parapubliques. Nous demandons ainsi au Conseil d'État de répondre aux questions suivantes :

1. *Des attaques informatiques ont-elles été constatées sur des collectivités publiques neuchâteloises ? Quelle est la probabilité d'un événement de ce type selon l'évaluation des risques effectuée par l'exécutif ?*
2. *La conseillère d'État en charge de la digitalisation indique dans l'édition du journal Le Temps du mercredi 25 août à ce propos que « le risque zéro n'existe pas ». Quelles sont les mesures prises par l'État pour limiter ces risques et garantir la sécurité informatique des collectivités publiques neuchâteloises, en particulier les données personnelles des habitant-e-s ?*
3. *Des audits du niveau de sécurité informatique du dispositif neuchâtelois sont-ils réalisés régulièrement ? Si oui, selon quelles méthodes et avec quels résultats ?*
4. *En cas de piratage, des directives sont-elles en place concernant la transparence et l'information aux catégories de la population concernées ?*

Le Conseil d'État peut-il certifier que l'ensemble des données des collectivités publiques neuchâteloises sont stockées sur le territoire neuchâteloise, voire suisse ?

Signataires : Antoine de Montmollin, Baptiste Hunkeler, Nathalie Ebner Cottet, Josiane Jemmely, Amina Chouiter Djebaili, Garance La Fata, Romain Dubois, Jonathan Gretillat, Fabienne Robert-Nicoud, Christian Mermet, Anita Cuenat, Corine Bolay Mercier, Sarah Fuchs-Rota, Hugo Clémence, Joëlle Eymann.

Réponse écrite du Conseil d'État, transmise aux membres du Grand Conseil le 22 septembre 2021

Préambule :

Le responsable sécurité des systèmes d'information (RSSI) du SIEN estime qu'il n'est pas opportun de communiquer publiquement sur les questions de sécurité informatique pour ne pas favoriser le hacking, plus particulièrement sur les mesures de sécurité mises en œuvre.

Le risque d'une cyberattaque réussie contre l'infrastructure informatique du SIEN doit être compris comme un risque systémique pour le canton de Neuchâtel.

1. **Des attaques informatiques ont-elles été constatées sur des collectivités publiques neuchâteloises ?**

   Il y a des milliers de tentatives d'exploitation des failles de sécurité qui sont bloquées chaque jour.

   Quelle est la probabilité d'un événement de ce type selon l'évaluation des risques effectuée par l'exécutif ?

   La probabilité d'un événement de ce type est élevée.

2. **La conseillère d'État en charge de la digitalisation indique dans l'édition du journal *Le Temps* du mercredi 25 août à ce propos que « le risque zéro n'existe pas ». Quelles sont les mesures prises par l'État pour limiter ces risques et garantir la sécurité**

informatique des collectivités publiques neuchâteloises, en particulier les données personnelles des habitant-e-s ?

La politique générale de sécurité des systèmes d'information (PGSSI) souligne l'engagement du Conseil d'État à soutenir les mesures visant à assurer une protection appropriée des systèmes d'information de l'Administration cantonale neuchâteloise (ACNE) et de ses partenaires conventionnés avec le SIEN contre toutes les menaces, qu'elles soient d'origine interne ou externe, accidentelles, environnementales ou délibérées.

Un ensemble de mesures de sécurité techniques et organisationnelles sont mises en œuvre par le SIEN selon les bonnes pratiques identifiées dans la norme ISO 27001, notamment une politique régulière de mise à jour des systèmes informatiques et une veille continue des alertes de sécurité en collaboration avec le Centre national pour la cybersécurité (NCSC).

Chaque solution de sécurité mise en œuvre pour l'administration cantonale neuchâteloise par le SIEN est aussi mise en œuvre pour les collectivités publiques neuchâteloises.

3. **Des audits du niveau de sécurité informatique du dispositif neuchâtelois sont-ils réalisés régulièrement ? Si oui, selon quelles méthodes et avec quels résultats ?**

Le canton de Neuchâtel participe régulièrement aux évaluations selon le standard NIST du Réseau national de sécurité (RNS). Lors de la dernière évaluation, le canton de Neuchâtel se classe dans le tiers supérieur des cantons suisses en ce qui concerne son dispositif de sécurité informatique.

Le SIEN réalise un rapport annuel ISAE3402 (International Standard on Assurance Engagements n°3402) permettant aux utilisateurs des prestations du SIEN d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de services.

Le CCFI réalise des audits conformément aux principes fondamentaux de contrôle, aux lignes directrices de l'INTOSAI, ainsi qu'aux normes internationales pour la pratique professionnelle de l'audit interne.

Les résultats des différents audits sont pris en compte, les corrections nécessaires sont effectuées.

En cas de piratage, des directives sont-elles en place concernant la transparence et l'information aux catégories de la population concernées ?

Si une perte de données est constatée, le SIEN suit sa politique de réponse aux incidents.

L'autorité concernée par la perte ainsi que le préposé à la protection des données et à la transparence du canton du Jura et de Neuchâtel sont informés au plus vite lors de la phase de détection. Si la nature de la perte nécessite une communication aux citoyens, une helpline est mise à disposition par le SIEN.

Suite à la phase de confinement et remédiation, la deuxième étape de l'analyse consiste à identifier la nature des données volées afin de pouvoir informer personnellement les citoyens concernés.

La troisième étape consiste à analyser plus finement les données volées afin d'identifier les données particulièrement sensibles qui peuvent nécessiter une action immédiate et de prendre les actions de mitigation appropriées.

Il n'est pas possible d'effacer les données sur le darknet.

Le Conseil d'État peut-il certifier que l'ensemble des données des collectivités publiques neuchâteloises sont stockées sur le territoire neuchâtelois, voire suisse ?

Nous pouvons confirmer que les données hébergées par le SIEN sont localisées dans le canton de Neuchâtel ou en Suisse.