REPONSE DU CONSEIL COMMUNAL A L'INTERPELLATION 25-603 DE M. NOLAN BONGIOVANNI INTITULEE « CYBERSECURITE ET PROTECTION DES DONNEES : ÉTAT DES LIEUX ET MESURES EN PLACE »

(Du 19 mai 2025)

Monsieur le Président,
Mesdames, Messieurs,

En date du 29 mars 2025, M. Nolan Bongiovanni, conseiller général indépendant, a déposé l'interpellation 25-603 intitulée « Cybersécurité et protection des données : État des lieux et mesures en place », inscrite pour la première fois à l'ordre du jour de la séance du Conseil général du 7 avril 2025 et dont le contenu est le suivant :

> *La cybersécurité représente aujourd'hui un enjeu majeur pour les administrations publiques et les institutions académiques. La transformation numérique de la Ville de Neuchâtel expose les infrastructures informatiques et les bases de données à des menaces croissantes.*
>
> *Les récents incidents, notamment l'attaque contre l'Université de Neuchâtel en 2022, ont mis en lumière la vulnérabilité des systèmes et l'importance d'une protection adaptée. Un simple hôpital peut subir plus de 200 attaques par jour, et certaines aboutissent à des compromissions critiques : vol ou falsification de données, altération ou suppression de bases de données, détournement d'accès, ou encore exploitation des journaux d'activité (logs).*
>
> *Dans ce contexte, nous interpellons le Conseil communal avec les questions suivantes :*

1) Audit et évaluation des risques

La Ville de Neuchâtel a-t-elle réalisé un audit approfondi de ses infrastructures informatiques pour identifier d'éventuelles failles de sécurité ? Un rapport a-t-il été produit sur les vulnérabilités détectées et les mesures correctives mises en place ?

2) Conformité aux normes et certifications de sécurité

Quelles normes et certifications en matière de cybersécurité sont actuellement appliquées par la Ville ? Les infrastructures respectent-elles des standards reconnus, tels que les recommandations du NIST ou la certification ISO 27001 (sachant que cette dernière est particulièrement exigeante) ?

3) Chiffrement et protection des données

Comment la Ville assure-t-elle la protection des bases de données et des documents sensibles ? Le chiffrement est-il appliqué au niveau des partitions de stockage pour éviter un accès non autorisé par des systèmes tiers ? Quels mécanismes de protection sont en place pour empêcher l'accès aux données en cas de compromission d'un serveur ?

4) Contrôle des accès et authentification

L'accès aux infrastructures informatiques repose-t-il sur une authentification multifactorielle (MFA) généralisée ou seulement sur les systèmes sensibles ? Un contrôle basé sur le secteur d'activité ou par application est-il prévu ?

5) Cellule dédiée à la cybersécurité

Existe-t-il une cellule spécialisée en cybersécurité au sein de l'administration communale ? Si oui, comment est-elle structurée et quelles sont ses missions principales ?

6) Plan de réponse en cas de cyberattaque

La Ville dispose-t-elle d'un plan de réponse en cas de cyberattaque aboutie ? Ce plan prend-il en compte des scénarios précis tels que le chiffrement malveillant des données (ransomware), le vol ou la falsification des bases de données, la suppression de données critiques ou encore la compromission des logs de sécurité ?

7) Coopération avec les autorités cantonales et fédérales

Une coopération active avec les autorités cantonales et fédérales en matière de cybersécurité est-elle en place ? Des ressources sont-elles mutualisées avec d'autres institutions pour renforcer la protection des systèmes informatiques locaux ?

8) Hébergement des données et souveraineté numérique

La Ville de Neuchâtel héberge-t-elle ses données sur des infrastructures situées en Suisse ou fait-elle appel à des services cloud étrangers ? Une migration vers des solutions d'hébergement souverain suisse est-elle envisagée pour garantir un meilleur contrôle des données communales ?

9) Sensibilisation et formation des employés

Des formations régulières en cybersécurité sont-elles proposées aux employés de l'administration communale et aux étudiants, notamment pour se prémunir contre les attaques de type phishing et ransomware ?

10) Investissements en cybersécurité et modernisation des infrastructures

La Ville prévoit-elle des investissements pour moderniser ses infrastructures numériques et anticiper les nouvelles menaces cybernétiques ?

Nous remercions le Conseil communal pour ses réponses à ces questions, qui visent à garantir une protection optimale des données et à renforcer la confiance des citoyens envers la sécurité des systèmes informatiques communaux.

1. Contexte

Votre Autorité, sur proposition de l'exécutif, a validé la fusion du Centre électronique de gestion (CEG), alors service communal, avec le Service informatique de l'Entité neuchâteloise (SIEN), service cantonal, avec effet au 1er janvier 2019. Depuis lors, l'informatique est gérée par le SIEN, par un mandat de prestation informatique.

C'est ainsi au niveau cantonal que la plupart des questions posées trouveront réponse. Cependant, la Ville, si elle délègue sa gestion

informatique au SIEN, est en contact fréquent avec son mandataire et s'assure du respect du cadre légal. A noter que le Canton et, partant, le SIEN, est soumis au même cadre légal que la Ville en termes de sécurité et de protection des données. Le Canton applique en outre une politique générale de sécurité des systèmes d'information (PGSSI) et une politique de sécurité des systèmes d'information (PSSI) strictes.

De plus, pour des raisons évidentes de sécurité, il n'est pas possible de dévoiler publiquement toutes les mesures de sécurité mises en place par le SIEN.

Le cadre de l'informatique communal étant fixé, nous pouvons vous faire part des éléments suivants.

2. Réponses aux questions

2.1 Audit et évaluation des risques

La gestion informatique étant du ressort du SIEN, c'est ce dernier qui fait l'objet d'audit sur les infrastructures informatiques.

Le SIEN fait réaliser un audit ISAE 3402 – Type 1 (International Standard on Assurance Engagements) chaque année par une société indépendante. Le rapport a confirmé que les contrôles conçus fournissent une assurance raisonnable quant à la fiabilité du dispositif de contrôle interne et des prestations de services.

Le SIEN organise des audits et des tests de pénétrations de façon ponctuelle sur certains systèmes d'informations (infrastructure, application et autres systèmes traitant de l'information). Parmi les autres mesures de sécurité notables mises en place aujourd'hui, les systèmes d'informations sont scannés mensuellement pour identifier les vulnérabilités existantes.

2.2 Conformité aux normes et certifications de sécurité

Un ensemble de mesures de sécurité techniques et organisationnelles sont mises en oeuvre 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).

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.

Un projet de certification ISO 27001 est en cours au SIEN afin de s'assurer un alignement aux meilleures pratiques. La posture de sécurité du canton est annuellement évaluée avec le standard NIST CSF 2.0.

2.3 Chiffrement et protection des données

Les bases de données et les informations sensibles sont protégées principalement par la segmentation des réseaux et une gestion des accès limités à qui de droit. Les stations de travail sont chiffrées avec Bitlocker.

2.4 Contrôle des accès et authentification

La double authentification n'est pas nécessaire sur le réseau câblé et sans-fil du SIEN. Depuis Internet, seuls les sites publics (Ville et institutions) sont accessibles sans authentification.

L'authentification multifactorielle est requise pour tout accès à un système d'information traitant des données non-public accessible depuis l'externe, lorsque celui-ci le permet. Ce contrôle n'est pas basé par secteur d'activité ou par application.

2.5 Cellule dédiée à la cybersécurité

Il n'existe pas de cellule spécialisée en cybersécurité au sein de l'administration communale, ce mandat est attribué au SIEN.

Le SIEN dispose d'un centre opérationnel de sécurité (SOC) dont les missions sont :

- Surveiller de façon continue (24/7/365) les systèmes d'information pour détecter, prévenir et répondre aux cybers incidents.
- Améliorer continuellement la posture de sécurité.
- Détecter les vulnérabilités et les risques de sécurité, organiser et suivre leur remédiation.

2.6 Plan de réponse en cas de cyberattaque

Là encore, la Ville s'en remet au SIEN qui est responsable des infrastructures et qui possède son plan de réponse.

Le SIEN dispose de plan de réponse en cas de cyber incident avéré. Ces plans comprennent notamment : la réponse aux rançongiciels, ingénierie sociale, fuites de données, dénis de service ou la compromission d'un partenaire externe. Cette réponse est assurée 24h sur 24, 365 jours par an, en collaboration avec une société externe.

Dans l'éventualité d'une cyberattaque, la « victime » de l'incident reste la principale responsable. Toutefois, la gestion de la réponse à l'incident se fait en étroite collaboration avec le SIEN. La direction de l'entité affectée et le SIEN travailleront de concert pour piloter les opérations de réponse. Le SIEN, grâce à sa cellule de crise, mettra en œuvre son protocole de gestion de crise afin de coordonner les actions avec l'entité affectée.

2.7 Coopération avec les autorités cantonales et fédérales

Comme expliqué en introduction et conformément à la politique générale de sécurité des systèmes d'information (PGSSI) du Conseil d'État, les partenaires conventionnés avec le SIEN collaborent activement à garantir la cybersécurité.

Le SIEN collabore étroitement avec l'office fédéral de la cybersécurité (OFCS) et les cantons latins pour partager ses expériences et renforcer la sécurité des systèmes d'informations. Les ressources en matière de cybersécurité sont mutualisées entre l'administration cantonale, les communes et le réseau de santé neuchâtelois.

2.8 Hébergement des données et souveraineté numérique

Par extension, selon les politiques déjà mentionnées, les données de la ville sont hébergées pour la majorité dans les infrastructures du SIEN et pour une petite partie dans des infrastructures suisses.

Le SIEN informe les responsables de traitement des données de leurs responsabilités au regard de la réglementation sur la protection des données. L'avis du Préposé à la protection des données et à la transparence Jura Neuchâtel est demandé lors de la mise en œuvre par le SIEN de solutions hébergées en dehors de ses infrastructures et traitant des données sensibles. L'analyse des besoins de protection dans les

projets prend en compte les questions en lien avec le respect des lois sur la protection des données.

Les collaborateurs-rices de la ville sont rendu-e-s attentifs-ves à leurs responsabilités dans le traitement et le stockage des données et quant à l'utilisation de solutions numériques conformément au cadre légal.

2.9 Sensibilisation et formation des employé-e-s

En mars 2023, une campagne de sensibilisation aux risques cyber a été réalisée auprès des employé-e-s de la Ville. Les résultats de la campagne ont démontré la nécessité de reproduire l'exercice, ce qui est prévu.

La formation des étudiant-e-s relève des établissements scolaires fréquentés.

2.10 Investissements en cybersécurité et modernisation des infrastructures

Le nouveau datacenter du SIEN a été inauguré récemment et est à la pointe pour garantir la sécurité, la disponibilité et l'intégrité des données.

La modernisation des équipements déployés à la Ville (postes de travail et équipements réseaux) se fait en accord avec le SIEN dans les budgets de fonctionnement.

3. Conclusion

La cybersécurité fait partie des enjeux traités quotidiennement par le SIEN qui gère avec diligence cet aspect essentiel de l'informatique en respectant des normes exigeantes.

La Ville bénéficie directement des compétences misent en œuvre et souhaite pour sa part poursuivre la formation et la sensibilisation du personnel, consciente que la sécurité et la protection des données de ses citoyens est l'affaire de toutes et tous.

Neuchâtel, le 19 mai 2025

AU NOM DU CONSEIL COMMUNAL:

La présidente,	Le chancelier,
Violaine Blétry-de Montmollin	Daniel Veuve