Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

focus 5/23
novembre

POINT FORT

Cybersécurité: unir nos forces et compétences

Natacha Litzistorf,
élue à la Municipalité de Lausanne, directrice du Logement, de l'environnement et de l'architecture.

Les cyberattaques sont de plus en plus nombreuses et sophistiquées et touchent de plus en plus d'acteurs, privés ou publics. Plusieurs affaires dans des communes ont été largement médiatisées, plus que celles dans le privé d'ailleurs et ont créé un réel électrochoc dans le monde politique... et c'est tant mieux. En effet, ces épisodes nous ont permis de prendre davantage conscience que « l'informatique, c'est une politique publique stratégique » et que la sécurité en est la pierre angulaire, avec la protection des données. Ces événements brutaux nous ont conduits à adopter une posture plus adéquate consistant à mettre plus de deniers publics dans le domaine, à faire preuve d'humilité car personne n'est à l'abri, à œuvrer de façon discrète, en évitant de révéler nos schémas tactiques tout en informant la population, mais surtout en collaborant et en échangeant entre les acteurs tant publics que privés.

Le 14 juin dernier, l'administration communale de Lausanne a constaté une attaque informatique visant les services exposés sur Internet. Un premier diagnostic a rapidement permis de déterminer que la Ville faisait face à une attaque de type Déni de service distribué (DDoS), avec pour principales conséquences l'indisponibilité de ses sites web. Le protocole d'urgence a été activé pour entres autres informer les parties prenantes et prendre les mesures adéquates en collaboration avec le Canton et la Confédération. Les actions coordonnées ont permis de baisser l'intensité des attaques pour protéger les serveurs et les données.

Avoir vécu cette attaque nous a permis de tirer des enseignements nouveaux mais aussi de confirmer des choses que nous savions déjà théoriquement. L'échange d'information entre les villes attaquées est essentiel. En période de crise, nous sommes tous et toutes le nez dans le guidon, occupés à rechercher des solutions. Il serait utile d'avoir « un outil » de coordination qui facilite les liens, tant au niveau politique qu'au niveau de l'administration. La communication demeure un élément clé : dans le système politico-administratif, elle est cruciale car tout le monde doit connaître son rôle et ses responsabilités. Avec le parlement, elle doit être prévue et s'insérer juste après l'interne. Au grand public, elle doit être transparente, tout en ne s'exposant pas aux malveillances à l'œuvre et sur les réseaux sociaux, les rumeurs doivent être démenties. Une évidence chapeaute le tout : être prêts reste la clé de la gestion de crise.

Mais le maillon sur lequel il faut insister fortement dans nos politiques de cybersécurité, c'est l'humain. En effet, c'est par une formation obligatoire et continue, tout comme par une information interne régulière que nous arriverons à sensibiliser aux enjeux et là encore, nous pourrions, au niveau des villes jouer la carte de la mutualisation. C'est à cette condition qu'un changement de culture s'opérera et que nous serons mieux préparés au cybermonde, toujours avec compétence, détermination et humilité.

Chère lectrice, cher lecteur

Dans un monde de plus en plus interconnecté où les technologies numériques dominent notre quotidien, la cybersécurité joue un rôle déterminant pour la sécurité et la stabilité des villes.

Les réseaux sociaux, la communication en ligne et la cyberadministration sont omniprésents dans la vie de la population et du personnel - et donc vulnérables aux cyberattaques. Il en va de même des infrastructures sensibles fortement numérisées telles que l'approvisionnement en eau et en électricité, les systèmes de transport et les établissements de santé.

Vu ce constat, les villes doivent investir dans la sécurité de leurs infrastructures numériques et sensibiliser leur personnel. Cette édition de «focus» s'interroge: Comment la Ville de Lausanne aborde-t-elle ce problème? Qu'en dit le responsable politique biennois? Et quelles sont les recommandations du Centre national pour la cybersécurité? Vous en saurez plus en lisant la présente édition de «focus».

Nous vous souhaitons bonne lecture!

Sommaire

INTERVIEW

« La sensibilisation ne suffit pas à elle seule »

Beat Feurer,
Conseiller municipal de la Ville de Bienne

Beat Feurer (UDC) est conseiller municipal (exécutif) de la Ville de Bienne. Élu au gouvernement municipal en 2012, il a été en charge de la Direction de l'action sociale et de la sécurité jusqu'en mars 2023.

Âgé de 63 ans, il est directeur des finances depuis avril 2023. Dans cette fonction, il est également responsable du Département informatique et logistique, et donc de la cybersécurité.

Selon vous, qui êtes le responsable politique en matière d'informatique, quelle est l'importance que revêt la cybersécurité?

Ces dernières années, cette thématique s'est développée et la Ville de Bienne a beaucoup investi dans ce domaine. Pour la gestion de la sécurité de l'information, nous suivons les recommandations de la norme ISO 27001.

Avez-vous déjà été victimes d'une cyberattaque?

Comme toutes les organisations, nous sommes quotidiennement victimes d'attaques. À ce jour, aucune n'a eu de conséquences importantes pour la sécurité de nos systèmes et des données qu'ils contiennent.

Êtes-vous bien préparés à une potentielle cyberattaque?

Ces trois dernières années, nous avons beaucoup investi dans ce domaine. Bien entendu, nous ne sommes jamais à l'abri, mais nous avons en tout cas pris les mesures nécessaires pour prévenir les attaques et réagir rapidement en cas de problèmes.

Quels sont les principaux enjeux pour protéger au mieux la Ville et sa population contre une nouvelle attaque potentielle?

De nos jours, le facteur humain demeure le risque prédominant. C'est pourquoi nous accordons une grande importance à la sensibilisation. Cependant, la sensibilisation ne suffit pas à elle seule; il est également essentiel de garantir que les membres de l'administration disposent d'outils sécurisés. Le déploiement rapide de ces outils est impératif pour contrer les menaces. Malheureusement, nos processus administratifs actuels ne sont pas toujours alignés avec les progrès technologiques, ce qui peut parfois entraver notre réactivité.

Quelles mesures concrètes ont été prises pour protéger les données de la population et l'infrastructure de la Ville contre des cyberattaques?

Nous travaillons sur les niveaux suivants :

- Établissement d'un cadre réglementaire solide pour la sécurité, comprenant des directives concernant la protection des informations et le traitement adéquat des données.
- Accompagnement des membres de l'administration par le biais de formations axées sur les risques liés à la sécurité de l'information, une sensibilisation grâce à la simulation d'attaques réelles, et la mise à disposition d'outils hautement performants.
- Mise en œuvre d'outils avancés pour surveiller nos systèmes, détecter les tentatives d'intrusion et réagir en cas d'attaque.
- Collaboration avec les autres administrations.

Comment se déroule la collaboration avec d'autres communes, avec le canton et la Confédération en matière de cybersécurité?

Nous collaborons étroitement avec l'ensemble des niveaux de l'administration, depuis les groupes d'échange intercommunaux jusqu'au soutien que nous recevons du Centre national pour la cybersécurité de la Confédération. Ces partenariats revêtent une importance capitale pour nous, car nous sommes conscients que travailler en solitaire dans ce domaine n'est pas envisageable.

Vu le nombre de menaces en hausse constante dans le domaine de la cybersécurité: Quelles stratégies ou quels plans l'administration de la Ville applique-t-elle pour garantir la cybersécurité de la Ville et se maintenir en permanence à la pointe du savoir-faire?

Protéger ses systèmes informatiques revient à connaître leur architecture et leur contenu aussi minutieusement qu'un ingénieur doit comprendre chaque détail d'un bâtiment et connaître son utilisation pour garantir sa sécurité. Nous avons donc lancé une initiative pour mieux documenter et connaître nos données, leur niveau de protection, leurs interfaces et leur qualité.

Avec l'évolution technologique actuelle, les administrations communales n'auront bientôt plus aucun système propriétaire. Toutes les applications seront disponibles uniquement dans des solutions dites « cloud » comme nous le connaissons déjà pour les utilisateurs privés. Cette évolution implique que nous devons maîtriser les flux d'informations qui transitent entre les machines de l'administration et les fournisseurs externes. C'est une condition sine qua non pour être capables d'appliquer une stratégie sécuritaire adéquate et de réagir rapidement en cas d'attaques des systèmes ou de perte de données.

THÈME

Cyberattaque – quels sont les bons réflexes?

Les cyberattaques et les pertes de données qui en résultent peuvent ébranler durablement la confiance de la population à l'égard de l'administration. Afin de s'en protéger de façon optimale, toutes les autorités et entreprises, et donc aussi les administrations des villes, devraient adopter une approche globale du thème de la cybersécurité et en faire un enjeu prioritaire. Il ne suffit pas d'en transférer la responsabilité à la seule personne responsable en matière d'informatique.

Sandra Lüthi
Experte en sensibilisation et prévention, Centre national pour la cybersécurité NCSC

En raison de leur activité publique, les collaboratrices et collaborateurs administratifs des villes se trouvent dans une position clé au sein de la chaîne de sécurité informatique. Ils travaillent avec des infrastructures informatiques et des outils qui leur permettent d'accéder, de saisir et de traiter des informations sensibles. Pour remplir leur mandat légal, il leur est indispensable d'enregistrer, de traiter et, dans certains cas, de transmettre diverses données personnelles concernant les habitantes et habitants, le personnel et les entreprises. Ils sont en outre quotidiennement en contact étroit avec des partenaires internes et externes via divers canaux de communication. Dans le cadre de leur activité, ils sont soumis au secret de fonction et tenus de traiter les affaires de service de manière confidentielle. En raison de la forte dépendance par rapport à l'infrastructure informatique, la liberté d'action d'une administration urbaine peut, en cas de cyberincident, se voir compromise rapidement, durablement et de manière à mettre en péril son mandat.

Quelques administrations urbaines, étant conscientes de ces enjeux, ont d'ores et déjà bien intégré le thème de la cybersécurité. Il en existe cependant d'autres qui nécessitent de rattraper le retard en la matière. Des lacunes peuvent notamment être constatées en ce qui concerne l'absence de mesures de sensibilisation, de formation, d'accords passés avec les prestataires de services informatiques et d'expérience pratique en matière de gestion d'une cyberattaque.

Préparation aux crises

Afin de vous préparer le mieux possible à un éventuel incident de cybersécurité, vous devriez réfléchir dès maintenant à la manière dont vous réagiriez à une situation de crise. C'est le seul moyen de savoir si vous êtes prêts en cas d'urgence. Définissez avec votre responsable informatique les consignes de sécurité minimales et contraignantes au niveau organisationnel, personnel et technique dans le domaine de la sécurité informatique. Clarifiez avec lui ou elle les processus et les responsabilités aussi bien en temps normal qu'en cas d'incident de cybersécurité. Consignez-les dans un plan de gestion continue afin d'assurer la continuité de vos activités.

Ce plan devrait également prévoir un concept de communication et de crise. Définissez en outre un contact d'urgence à joindre en cas d'incident de cybersécurité. Vous trouverez d'autres recommandations concernant la collaboration avec les prestataires de services informatiques sur le site Web du Centre national pour la cybersécurité (NCSC) sous le bouton «Informations pour les autorités» dans la rubrique «Thèmes actuels» . Un autre aspect d'une haute importance réside dans la sensibilisation et la formation des collaboratrices et collaborateurs. Des moyens actuels de sensibilisation sont présentés sur le site Web de la campagne annuelle de sensibilisation à la cybersécurité S-U-P-E-R.ch. Vous avez en outre la possibilité de demander l'accès à la nouvelle formation en ligne du Réseau national de sécurité (RNS). Pour ce faire, veuillez vous adresser à info@elearningcyber.ch. Par ailleurs, le cours EBAS destinés aux PME pourrait intéresser les administrations de petite et moyenne taille: www.ebas.ch/kmucourse.

Limitation des dommages en cas de cyberattaque

Lorsque survient une cyberattaque, il est important d'agir rapidement.

--Débranchez immédiatement les systèmes infectés par des logiciels malveillants du réseau. À cette fin, retirez le câble réseau de l'ordinateur et déconnectez le cas échéant les adaptateurs WLAN.
- Afin d'éviter toute propagation, interrompez les connexions Internet (Web, e-mail ainsi que les accès à distance et les accès VPN de chaque site).
- Vérifiez les sauvegardes de vos données et protégez-les immédiatement..
- Les sauvegardes doivent être au plus vite déconnectées physiquement du réseau infecté («mises offline»)
- **En cas de cyberattaque**, changez immédiatement les mots de passe. Dans les comptes de messagerie, vérifiez les éventuelles règles de transfert.

Contacter / déclarer / informer

- Alertez votre contact à joindre en cas d'urgence informatique.
- Réfléchissez à la question de savoir s'il convient de contacter la police et de porter plainte. Ne relancez pas les systèmes avant que la police ait relevé les indices.
- Le personnel de la police vous conseille et vous soutient dans la marche à suivre, il relève les indices et procède aux investigations. Informez la police via le numéro d'urgence 117.
- Déclarez l'incident au **NCSC** via le formulaire en ligne: www.report.ncsc.admin.ch.
- En cas de **vol de données** (p. ex. lors de rançongiciels), nous vous conseillons d'informer les personnes concernées de manière proactive. Clarifiez la question de savoir s'il existe une obligation légale de déclaration. Selon la nouvelle **loi sur la protection des données**, les violations de la sécurité des données doivent être déclarées auprès du PFPDT (art. 24 nLPD et art.15 LPDS). Pour ce faire, utilisez le formulaire en ligne: https://databreach.edoeb.admin.ch/report.

Pour en savoir plus

- Protégez votre autorité (admin.ch)
- Informations complémentaires/liens

Impressum
Éditeur: Union des villes suisses (UVS), Monbijoustrasse 8, Case postale, 3001 Berne. Téléphone: 031 356 32 32, www.uniondesvilles.ch. S'abonner au «focus»: info@staedteverband.ch
Rédaction UVS: Nathanël Bruchez, Marc Moser. **Images:** p 1: Rolf Siegenthaler; portraits pages 1.2 et 3: màd.