Les communes face aux défis de la cybersécurité

La place grandissante de l'informatique dans les communes soulève avec acuité la question de la protection des systèmes et données informatiques. Le Label cyber-safe.ch entend aider à gérer les cyberrisques de façon pragmatique.

Il est difficile pour une commune de savoir combien pourrait lui coûter un problème de sécurité informatique. Un exemple peut aider à éclairer la question: en cas de perte définitive des données relatives aux amendes d'ordre en cours, combien cela coûterait-il? Photo: Shutterstock

La pandémie de coronavirus nous offre (au moins) deux enseignements en matière de sécurité informatique. Premièrement, elle nous rappelle à quel point nos sociétés sont toujours plus dépendantes des systèmes informatiques, le recours massif au télétravail en étant une illustration. Deuxièmement, lorsque la crise est là, il est trop tard pour s'y préparer. Dès lors, les dispositions prises en amont d'une crise sont cruciales afin de l'affronter au mieux le jour où elle surgit. Derrière la trivialité apparente de ces enseignements se cache néanmoins une réalité plus complexe: quel est le niveau de sécurité informatique de votre commune, quels sont vos risques et, plus encore, quelles mesures prendre pour réduire les risques à un niveau acceptable? C'est précisément pour aider les communes et autres petites et moyennes organisations à répondre de façon pragmatique à ces questions que le Label cyber-safe.ch a été développé par l'Association Suisse pour le Label de Cybersécurité (ASLaC).

La question de la sécurité ne dépend pas de la taille d'une commune

Aujourd'hui, l'informatique occupe une place grandissante dans les activités des communes en s'étendant de la gestion des chaufferies communales aux stations d'épuration, en passant par la cyberadministration. De ce fait, quels que soient leur taille et leurs moyens, les communes ne peuvent plus éviter la question de la sécurité informatique. En effet, en cas de négligence, les risques encourus sont grands: fuites de données, vols d'informations ou encore interruptions de services d'importance critique pour la population. Avec au final pour conséquences des pertes financières, une image ternie de l'administration communale et, dans l'ensemble, un moins bon service aux citoyennes et citoyens.

Les communes face à des défis très concrets de la cybersécurité

Les communes font face à de nombreux obstacles en matière de sécurité informatique. Manque de compétences spécialisées en interne, complexité croissante des systèmes d'informations, coûts des audits et prestations de sécurité informatique ou encore absence de définition claire des rôles et responsabilités en matière d'informatique, tels sont les défis auxquels les administrations communales sont confrontées.

Dans un tel contexte, il est difficile pour une commune de savoir combien pourrait lui coûter un problème de sécurité informatique et, partant, d'évaluer les bénéfices des investissements visant à l'améliorer. Quelques questions peuvent ici offrir un premier éclairage: en cas de perte définitive des données relatives aux amendes d'ordre en cours, combien cela me coûterait-il? Quelle est la base de données la plus importante pour ma commune et si je la perdais, combien de jour-homme me faudrait-il pour la reconstituer? Si ces questionnements doivent permettre de dresser une première évaluation coûts/bénéfices de la cybersécurité, une réflexion d'ensemble autour des questions de sécurité informatique reste primordiale: qui est en charge de cette thématique? Quelles sont les données collectées? Qui peut y avoir accès et où sont-elles stockées? Sont-elles sauvegardées, et si oui, où le sont-elles et combien de temps faut-il pour les récupérer? Voici quelques-unes des questions auxquelles les administrations communales et élus sont confrontés.

Démarche participative, expérience-pilote auprès de communes vaudoises

Afin d'être sûr de répondre aux attentes des petites et moyennes organisations, l'ASLaC a réuni autour de la table représentants des autorités publiques, d'associations faîtières de l'économie, ou encore des hautes écoles et spécialistes en sécurité informatique. Ensemble, ils ont élaboré et coconstruit une série d'exigences à satisfaire pour l'obtention du label. Ces exigences portent sur l'infrastructure informatique, l'identification des mails frauduleux, ou des mesures organisationnelles (par exemple, la protection des données ou la gestion des sous-traitants). La jeune association, qui est membre du comité de pilotage de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), a en parallèle, mis en place une expérience-pilote avec l'Union des Communes Vaudoises. Si le pilote est encore en cours à l'heure actuelle, les résultats intermédiaires montrent que des failles critiques existent auprès de deux tiers des communes candidates et que, dans l'ensemble, la démarche leur permet d'obtenir une connaissance fine de leur situation, d'initier une réflexion stratégique ou encore de justifier les demandes de budget. Un soutien donc bienvenu pour les communes à l'heure de la cybersécurité.

Christophe Hauert
Membre fondateur de l'Association Suisse pour le Label de Cybersécurité

Infos:
www.cyber-safe.ch.

Le Label cyber-safe.ch

La première étape du processus de labellisation consiste à remplir un questionnaire gratuit sur www.cyber-safe.ch. En cas d'intérêt à poursuivre la démarche, la commune reçoit la visite d'un expert pour réaliser des scans réseaux et identifier les éventuelles failles. L'association collecte ensuite les adresses e-mail des collaborateurs et effectue des tentatives de phishing. Sur cette base, la commune reçoit un rapport chiffrant la valeur des données et risques encourus, ainsi que la liste des mesures de corrections à mettre en œuvre. Lorsqu'elle s'estime prête, un auditeur vient vérifier si les mesures préconisées ont été appliquées correctement et donne recommandation d'attribuer ou non le label.

Afin de garantir l'indépendance et la crédibilité du label, l'association et les auditeurs s'engagent à ne vendre aucune mesure corrective aux organisations candidates, conservant ainsi strictement son rôle de conseil impartial et indépendant.

Le label reste valable deux ans, durant lesquels l'organisation labellisée a accès à des services continus (tests de vulnérabilité et phishing) pour assurer le maintien du niveau de sécurité. Quant au prix, il est proportionnel au nombre de postes de travail et débute à environ 3000 francs pour une petite commune.

Christophe Hauert, membre fondateur

Christophe Hauert (1978) est titulaire d'un doctorat en Science Politique et travaille depuis plus d'une dizaine d'années dans la normalisation internationale et européenne. Après avoir été chargé de projet au sein d'une plateforme visant à renforcer l'implication des parties prenantes à l'élaboration des normes (INTERNORM), il a travaillé en tant que conseiller politique pour une organisation européenne où il a défini et mis en œuvre la stratégie de l'organisation en matière d'élaboration des normes européennes et internationales. Il a aussi enseigné en tant que chargé de cours à l'Université de Lausanne et a dispensé de nombreuses formations à l'échelle suisse et européenne sur les dimensions techniques et politiques de la normalisation. Il a le statut de membre associé auprès du CRHIM de l'Université de Lausanne et est également membre de l'Association suisse de normalisation (SNV).