9 conseils pour

Maintenir les services publics en cas de cyberattaque

La cybersécurité, c'est important. Mais comme le décrit très bien l'auteur de « Cyberattaque : assurer la continuité des services publics locaux », Lionel Pérès, mille excuses nous viennent pour repousser ce chantier. Pourquoi ? « On ne sait pas par où commencer ». Suivez le guide !

1 Penser la vie sans informatique

« La sérénité naît d'être prêt, pas d'être chanceux », philosophe Lionel Pérès, directeur général des services (DGS) de Vaison-la-Romaine (Vaucluse). Pour se rendre compte de la capacité d'un collectif à réagir à une cyberattaque, l'exercice immédiat et parlant est… le retrait des ordinateurs. Imaginez un instant que tous les systèmes informatiques d'une collectivité tombent en panne. Que se passe-t-il pour la gestion des eaux ? Des transports publics ? Des déchets ? Comment une famille peut-elle vérifier l'emplacement d'un caveau familial ? Et comment se fait le suivi d'une demande de place en crèche ? La conséquence immédiate d'une cyberattaque sur un système, c'est son arrêt. Sans préparation, cela peut être pire.

2 Connaître les fragilités intrinsèques aux collectivités

Les collectivités sont des cibles privilégiées, car elles gèrent à la fois des données sensibles et des services essentiels. Selon la « Synthèse de la menace », rapport publié le 24 février 2025 par l'Agence nationale de sûreté et de sécurité informatique (Anssi), les collectivités sont principalement la cible d'attaques à but lucratif car elles sont connues pour leur faible sécurité informatique et pour gérer des systèmes d'information disparates, difficiles à cartographier.

3 Suivre l'évolution du cadre légal

La directive européenne NIS 2 (Network and Information Security 2) sera transposée en France par la loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Le projet de loi, approuvé au Sénat le 12 mars 2025, est en cours d'examen à l'Assemblée nationale. Elle s'imposera aux communes de plus de 30 000 habitants et à toutes les intercommunalités. Le directeur de l'Anssi, Vincent Strubel, expliquait lors du forum InCyber de 2025 que la « NIS 2 est une nécessité. C'est l'occasion de parler de cybersécurité aux petites structures avant que des attaquants ne leur en parlent de manière moins agréable ».

4 Structurer son projet

Pour obtenir le soutien des élus et de la direction d'une collectivité, il est essentiel de structurer un projet clair et réaliste. Les postes obligatoires : un délégué à la protection des données (DPO) qui peut être mutualisé et un référent cybersécurité. Une formation basique des agents et élus est également nécessaire. Deux registres doivent être tenus. Un premier pour les activités de traitement de données personnelles et un second pour les violations de données constatées. Il faut aussi suivre les mises à jour logicielles et maintenir des sauvegardes fonctionnelles et testées régulièrement. Un document est indispensable : la politique de sécurité du système d'information (PSSI). On peut l'accompagner d'un plan de continuité d'activité pour le risque cyber (PCA-Cyber) et d'un plan de reprise d'activité (PRA-Cyber).

5 Constituer un comité de pilotage

Après avoir désigné un référent cybersécurité, il convient d'élargir le cercle des personnes impliquées en constituant une instance de gouvernance collective : le comité de pilotage. Il coordonne la démarche, arbitre les choix organisationnels et s'assure que les objectifs sont atteints. La présence de l'autorité territoriale est intéressante pour une première réunion, afin de légitimer la démarche, mais n'est pas nécessaire en tant que membre du comité. Les membres sont généralement un élu référent, le DGS, le DPO, le référent cybersécurité et un représentant des utilisateurs finaux. La répartition entre élus et administration doit se faire avant la première réunion. Les frustrations potentielles de personnes souhaitant participer au comité seront atténuées par la création immédiate d'un groupe de travail pour la conception du PCA-Cyber.

6 Prévoir la politique de sécurité du système d'information (PSSI)

La PSSI définit des règles claires et pédagogiques pour assurer la sécurité informatique. Ce n'est pas une charte. Elle s'apparente plutôt à un règlement intérieur des données et de l'informa-

tique. Elle est délibérée en conseil municipal et il est intéressant d'y inclure des règles d'hygiène informatique afin de sensibiliser les utilisateurs aux bonnes pratiques de sécurité. Une PSSI simplifiée, sans prestataire, est adaptée aux petites collectivités. Les bonnes pratiques lors de la manipulation de données sensibles et les choses à faire en cas de cyberattaque sont conservées.

7 Organiser une cellule de crise

Lors d'une cyberattaque, la collectivité est accompagnée. Les premiers gestes peuvent être importants (débrancher la machine d'internet, ne pas éteindre l'appareil, alerter le personnel, déposer plainte), mais très vite gendarmerie, région ou prestataires prennent la main pour gérer la crise informatique. « La collectivité attaquée a le statut de victime et c'est également le cas dans l'opinion publique », juge Lionel Pérès. « En 2020, on considérait encore la victime d'une attaque comme responsable de son sort. Ce n'est plus le cas. On sait que cela peut arriver à n'importe qui ». Ce que la collectivité doit gérer, c'est finalement ce qu'elle doit faire quelle que soit la crise. Et pour cela, elle doit identifier une cellule de commandement, une cellule terrain et une cellule communication. Notons que le dépôt de plainte est obligatoire pour l'intervention de l'assurance et qu'une déclaration doit être faite auprès de la Commission nationale de l'informatique et des libertés (Cnil) et de l'Anssi.

8 Mettre en place un PCA-Cyber

Un PCA est le balisage pour assurer la résilience des services publics en cas de cyberattaque. Il définit les mesures à prendre pour maintenir les services essentiels et minimiser les perturbations. Un PCA est donc différent d'une structure à l'autre. Dans ce document, chaque service est identifié par sa fonction, ses supports informatiques et les façons de continuer à le faire fonctionner sans ces supports. Cette approche permet à chacun de contribuer efficacement à l'identification des activités critiques et des solutions de continuité de son service, sans nécessiter d'expertise particulière en analyse des risques. C'est de cette façon que l'on se rend parfois compte qu'un vélo peut être nécessaire pour un réseau d'eau. Car si les capteurs ne transmettent plus l'information, il faut parfois aller faire des relevés dans des lieux inaccessibles en voiture.

9 Sensibiliser toutes les personnes concernées

Une fois le PCA-Cyber construit, il faut le mettre en œuvre et l'évaluer. Ce déploiement s'accompagne de la mesure la plus importante : la sensibilisation de toute personne qui a accès aux systèmes d'information. Maire, adjoint, agents de terrain, etc. Cet accompagnement commence par une note interne relative à la modernisation des systèmes d'information. Quelques jours plus tard, elle est suivie d'une séance de sensibilisation collective. Ce n'est qu'à partir de ce moment-là que l'on met en place les outils, comme la double authentification ou les gestionnaires de mots de passe. Pourquoi si tard ? Car sans la mise en place du comité, du PSSI, du PCA-Cyber et de la note interne, « on a simplement l'impression que les gens de la SI se sont levés ce matin avec une nouvelle lubie », plaisante Lionel Pérès. En mettant en œuvre cette démarche de quelques points, cent jours dans le livre de l'auteur, on cherche à ce que ce soit les utilisateurs eux-mêmes qui viennent demander une solution pour conserver tous leurs mots de passe. | ***Par Baptiste Cessieux***

Pour en savoir plus

« Cyberattaque : assurer la continuité des services publics locaux », Lionel Pérès, Territorial Éditions, 2025. Ce guide pratique propose des solutions accessibles et opérationnelles, adressées spécifiquement aux élus et dirigeants territoriaux. Il met l'accent sur les collectivités qui n'ont pas d'agents ou de services dédiés à la cybersécurité.