GESTION DE CRISE

Arthaz-Pont-Notre-Dame VICTIME D'UNE CYBERATTAQUE

La commune (1 657 habitants, Haute-Savoie) a été la cible de hackers en juin 2023. L'intégralité des données RH de la municipalité a été perdue. PAR **LUCILE BONNIN**

Lundi 12 juin 2023, les agents de la mairie d'Arthaz-Pont-Notre-Dame (74) découvrent que les données de la commune ont fait l'objet d'une cyberattaque par rançongiciel. Trois mois de travail ont été perdus.

« *On arrive un matin et il n'y a plus rien… Ça fait un drôle d'effet !* », raconte Julie Ruffet, secrétaire générale de mairie d'Arthaz-Pont-Notre-Dame. Pendant le week-end du 10 et 11 juin 2023, en effet, la petite commune a été victime d'une cyberattaque. Sur place, lundi 12 juin, au matin, impossible pour les agents d'ouvrir leurs sessions sur les ordinateurs. Après avoir contacté le prestataire informatique de la commune, la réponse de ce dernier est tombée comme un couperet : un logiciel malveillant a bloqué le système informatique de la commune en chiffrant ses données, c'est-à-dire en les cryptant. Les hackers demandent à la commune de payer une rançon de 30 000 dollars en bitcoin pour qu'elle récupère ses données, sans garantie. Ce mode opératoire s'appelle le rançongiciel. Les collectivités sont de plus en plus visées par ce type de menace (virus ou logiciels malveillants) avec une hausse des victimes de 36 % en 2023 par rapport à 2022, selon cybermalveillance.gouv.fr

Les petites communes sont loin d'être à l'abri. Il n'était évidemment pas question pour la commune de payer cette rançon. Une fois tous les ordinateurs éteints, son prestataire informatique a commencé le travail de nettoyage des virus, de réinstallation des systèmes et de récupération des données sauvegardées. Cette opération a été réalisée dans le cadre du contrat qui reliait le prestataire à la commune et ce, sans dépassement de coût.

Pendant trois semaines, les services informatiques de la mairie ont été perturbés par cette attaque. « *Cela a été vraiment long pour récupérer les données de la mairie et ce fut compliqué pour les agents de travailler correctement et sereinement* », raconte Régine Mayoraz, la maire de la commune. Finalement, les données de la municipalité ont pu être récupérées mais elles n'avaient pas été mises à jour depuis trois mois. Résultat : « *il a fallu reprendre tout le travail sur cette durée : la comptabilité, les salaires, les budgets, les arrêtés, l'état civil, les élections…* », témoigne Julie Ruffet. Certaines données liées à la comptabilité ont aussi été perdues, notamment toutes les informations rattachées aux titres et mandats émis « *comme les factures, les RIB des sociétés ou les certificats administratifs* ».

« UNE PERTE LOURDE »

De même, l'intégralité des données relatives à la gestion du personnel a été perdue. La commune compte une vingtaine d'agents et d'élus. C'est donc « *une perte lourde pour la commune* », regrette la maire. « *Heureusement, on a encore tendance dans les mairies à imprimer pas mal de documents pour les faire signer aux agents* », souligne la secrétaire générale de mairie. Mais elle constate cependant que la cyberattaque a encore une incidence aujourd'hui : « *Il arrive, presqu'un an après les faits, de devoir aller rechercher un document dans les dossiers papiers et c'est un peu lourd.* »

La commune n'avait pourtant pas lésiné sur les moyens pour protéger et sauvegarder ses données. Elle disposait déjà d'une sauvegarde interne en mairie, d'une autre dans un data center à Strasbourg, et d'une autre à Thonon-les-Bains. « *Après cette attaque, la préfecture nous a incité à faire un audit informatique pendant l'été 2023 et à changer de prestataire au profit d'un autre certifié par l'État* », explique la maire qui a confié la réalisation de l'audit à une société privée. Absence d'un accès « invité » sur la borne wifi de la mairie, manque d'antivirus sur les postes de l'école, sauvegarde trimestrielle des données au lieu d'une sauvegarde quotidienne : fort des enseignements de cet audit, le conseil municipal a décidé d'investir pour sécuriser au maximum les données de la mairie.

À la fin de 2023, la commune a changé de prestataire informatique. Le montant du contrat est quasiment multiplié par trois. Un coût de fonctionnement loin d'être négligeable pour la commune mais qui, espèrent élus et agents, portera ses fruits si la commune est une nouvelle fois attaquée ou qu'un incendie se déclare dans la mairie ou dans un centre de données.

© Facebook Arthaz Pont Notre Dame

Interview

Régine Mayoraz,

MAIRE D'ARTHAZ-PONT-NOTRE-DAME (74)

« CETTE ATTAQUE A ÉTÉ UNE VRAIE SURPRISE »

© Mairie d'Arthaz-Pont-Notre-Dame

● Vous attendiez-vous à être, un jour, une cible pour les cybercriminels ?

On était loin de s'imaginer cela. Notre commune n'est ni particulièrement grande, ni particulièrement riche. Je ne voyais pas vraiment l'intérêt qu'auraient pu avoir des cybercriminels à nous attaquer. Pourquoi notre commune ? Je pense qu'il n'y a pas vraiment d'explication. Il est certes plus facile aussi d'attaquer une petite mairie qu'une grande entreprise par exemple. Mais cette attaque a été une vraie surprise.

● Quels enseignements avez-vous tiré de cet épisode ?

Il est difficile pour une petite commune comme la nôtre de lutter contre les cyberattaques. Nous n'avons pas d'informaticien en interne, on ne s'y connaît pas en informatique et on doit donc faire totalement confiance à notre prestataire. Cette dépendance nous oblige à rester vigilants sur ce que ce dernier met en place. Nous n'avons pas hésité à changer de prestataire informatique.

Au niveau des agents, il y a une méfiance qui s'est développée naturellement au niveau des pratiques informatiques. On fait moins attention quand on n'a jamais rien eu mais une fois que ça arrive, on est plus attentifs.

● Que conseillez-vous aux petites communes pour gérer au mieux une cyberattaque ?

Il ne faut pas payer la rançon. Ensuite, pour faire face à la crise, il faut essayer de bien s'entourer, aussi bien au niveau du prestataire informatique qu'avec d'autres acteurs comme le délégué à la protection des données (DPO).

La communication est aussi un point essentiel. Quand on a su qu'on avait perdu les données « RH », on a informé tout le personnel pour que les agents puissent faire attention à leurs comptes bancaires. Ils ont notamment apprécié qu'on les prévienne et aucun souci n'a été constaté par la suite.

Les acteurs clés

GENDARMERIE. Après avoir prévenu le prestataire informatique, la maire, Régine Mayoraz, a été porter plainte auprès de la gendarmerie. Cette étape est essentielle pour lutter contre la cybercriminalité. Certains gendarmes sont aussi formés pour accompagner les communes dans la mise en place d'un service de sécurité.

ASSOCIATION DÉPARTEMENTALE DE MAIRES. La maire a très vite contacté l'Association des maires de Haute-Savoie pour connaître la marche à suivre et pour prévenir les autres mairies du département de cette attaque qui aurait pu potentiellement toucher d'autres communes.

DPO. La commune a fait appel à sa déléguée à la protection des données (DPO) externalisée qui a déclaré la violation de données à la CNIL dans le délai réglementaire de 72 heures (lire www.mairesdefrance/2769) et prévenu la préfecture.

CYBERMALVEILLANCE.GOUV.FR L'Association des maires de Haute-Savoie a incité la commune à faire une déclaration sur le site cybermalveillance.gouv.fr afin de recevoir des conseils adaptés. Ce groupement d'intérêt public propose un outil de diagnostic en ligne et une éventuelle mise en relation avec des professionnels pour une remédiation de l'incident.

Recourir à un expert de la sécurité numérique

Est-ce que le prestataire est compétent dans le champ de la sécurité informatique et peut réagir en cas d'attaque cyber ? C'est une question qu'il faut se poser. Le label ExpertCyber peut aider les communes à identifier des prestataires qualifiés. Créé par le groupement d'intérêt public (Gip) Cybermalveillance.gouv.fr, *« ce label permet de valoriser les entreprises de services informatiques justifiant d'une expertise en sécurité numérique sur les volets d'installation, de maintenance et d'assistance, et ainsi d'apporter aux bénéficiaires une meilleure lisibilité de la qualité d'offre de services pour être accompagnés dans un cadre de confiance »*. Sur le site cybermalveillance.gouv.fr, un annuaire des professionnels labellisés est mis à disposition des communes. Il suffit de saisir le nom d'un prestataire en cybersécurité pour vérifier s'il est labellisé ExpertCyber.