

COMMUNIQUÉ DE PRESSE

CYBERATTAQUE CONTRE L'ADMINISTRATION ROLLOISE – MESSAGE DE LA MUNICIPALITÉ

ÉTAT DES LIEUX AU 29 AOÛT 2021

Rolle, le 29 août 2021 – La Municipalité de Rolle informe de l'avancée des travaux de la task force mise en place pour gérer les suites de la cyberattaque dont elle a été victime le 29 mai dernier (voir chronologie des faits ci-après). Avec l'aide du Centre opérationnel de sécurité (SOC) de l'État de Vaud et d'experts en cybersécurité, sa première mission est d'analyser les données volées afin de pouvoir en informer personnellement les citoyens concernés. Elle appelle la population à la plus grande vigilance sur toute tentative de fraude qui pourrait survenir, principalement par téléphone ou email.

À l'instar de nombreuses institutions publiques ou privées d'envergure, l'Administration de Rolle a été victime d'une attaque de ses systèmes informatiques par un groupe international de cybercriminels.

L'état des lieux au dimanche 29 août est le suivant :

Le 25 août, une task force a été constituée comprenant la Municipalité *in corpore*, la cheffe de service en charge de l'informatique et des finances, le secrétaire municipal, le directeur de la sécurité numérique de l'État de Vaud et un spécialiste en communication. Elle est opérationnelle et se réunit tous les jours depuis le 26 août.

Avec l'aide du Centre opérationnel de sécurité (SOC) de l'État de Vaud et d'experts en cybersécurité, sa première mission est d'analyser les données volées afin de pouvoir informer personnellement les citoyens concernés, en concertation avec l'Autorité de protection des données et de droit à l'information du Canton.

Les experts ont récolté toutes les données découvertes à ce jour sur le darknet. Une première étape d'analyse a permis d'identifier le type de données disponibles (email, formats des documents, présence de liens, etc.). Selon les estimations de ce jour, cela représente environ 32 Go (soit 1,6 % de la quantité totale de données que possède la Commune) dont 64 boîtes emails.

Le 2^e niveau d'analyse, déployé avec l'aide du Canton de Vaud, doit permettre d'indexer les données selon leur niveau de sensibilité afin de pouvoir indiquer quels habitants ou entités sont directement concernés et, par la suite, de pouvoir leur communiquer les informations qui seraient compromises. Ce travail est complexe, car, hormis le volume de données concerné, leur format est très hétérogène et nécessite un travail manuel important, donnée par donnée. En dépit des moyens engagés, il n'est en conséquence pas possible de dire aujourd'hui la date à laquelle les résultats de ces travaux seront disponibles.

À relever qu'il est malheureusement impossible d'effacer ni d'empêcher l'accès aux données déposées sur le darknet, créé justement pour empêcher la localisation des serveurs sur lesquels les données ont été déposées.

Les experts consultés estiment que de tels vols de données induisent rarement des risques directs. Elles représentent en revanche un potentiel pour des personnes malveillantes, notamment sous la forme de tentatives de fraude et d'usurpation d'identité. La Municipalité agira par toute voie de droit utile afin que cesse tout traitement illicite ou préjudiciable des données.

Une priorité sera de détecter les données bancaires qui ont été échangées avec la Commune. Nous invitons les citoyens et entreprises qui pourraient être concernés à contacter la helpline qui sera mise en place afin de cibler les recherches et d'accélérer les réponses personnalisées.

L'essentiel des tentatives malveillantes proviennent par email ou par appels téléphoniques d'émetteurs inconnus. Une vigilance accrue est demandée à la population envers toute sollicitation suspecte afin d'éviter des clics inappropriés sur des liens ou des pièces jointes douteuses ainsi que la divulgation d'informations telles que mots de passe ou encore des versements indus.

Le site web de la Commune va s'habiller d'une page dédiée à la cyberattaque dès la semaine prochaine et relayera régulièrement l'avancement des travaux d'analyse.

Rappel de la chronologie des faits

Dans la nuit du samedi 29 au dimanche 30 mai 2021, en dépit d'un niveau de sécurité jugé adéquat par notre prestataire informatique, une cyberattaque a visé les systèmes informatiques de notre Commune. À l'aide d'un maliciel, les pirates ont chiffré l'intégralité des données qui y étaient conservées et dérobé un volume – estimé selon les analyses qui ont pu être effectuées par la suite – correspondant à environ 1,6 % du total de nos données.

Dès le dimanche 30 mai, avec le support de la Computer emergency response team de la Confédération (GovCERT), de la Police cantonale vaudoise et d'une société spécialisée en cybersécurité, les données compromises ont pu être intégralement vérifiées et restaurées à partir d'une copie de sauvegarde sur un serveur externe. Grâce à cette prise en charge immédiate, diligente et concertée, nos systèmes informatiques ont ainsi été sécurisés en deux semaines. Cette opération s'est déroulée sans céder à la demande de rançon des cybercriminels et notre dispositif de protection a encore été renforcé selon les recommandations émises par nos partenaires. Une plainte pénale contre X a été déposée le 14 juin.

Afin de ne pas attirer l'attention sur la vulnérabilité de la Commune ni sur des données exfiltrées non identifiées, aucune communication grand public n'a été faite à ce moment-là, suivant en cela la recommandation de nombreux experts en cybersécurité.

Le 24 juin, notre service informatique a reçu par email un message de la GovCERT l'informant que les données volées lors de la cyberattaque avaient été repérées sur le darkweb. Nous avons alors contacté la Police cantonale et la Protection des données du Canton afin de déterminer leur niveau de sensibilité et demandé à l'ensemble du personnel concerné par les piratages d'emails de vérifier et de changer leurs mots de passe.

Sans protocole d'action ni outils *ad hoc* au sein des communes vaudoises et par manque d'expérience, le risque lié à ce que pouvaient représenter des documents non identifiés déposés sur le darknet a été sous-estimé. La restauration complète et rapide de nos systèmes sans compromission vis-à-vis de pirates informatiques a contribué à nourrir le sentiment que le problème était résolu et aucune action d'urgence n'a été entreprise.



Des articles parus dans Watson puis dans Le Temps mercredi 25 août ont permis à tous de prendre conscience de la nature des données volées et de leur accessibilité. Ce même jour, la Municipalité a tenu une séance de crise avec des spécialistes et annoncé par voie de communiqué 6 mesures que nous vous détaillons ci-dessous :

1. Une **task force** a été constituée. Elle est opérationnelle et sa première mission est d'analyser les données volées et de convenir de la suite à donner vis-à-vis de la population, en concertation avec l'État de Vaud et l'Autorité de protection des données et de droit à l'information.
2. Une **helpline** sera accessible à tous rapidement. Son rôle sera en particulier de recueillir les demandes spécifiques des citoyens par rapport à leurs données.
3. Des **séances d'information** et de conseils pragmatiques pour la population seront mises sur pied courant septembre avec un expert de référence en matière de sécurité numérique. Ces présentations incluront un temps de questions/réponses.
4. Un **programme de prévention** ciblé sur la cybersécurité pour nos collaborateurs et l'actualisation de notre charte informatique sera mis en route dès le mois de septembre.
5. Des **audits** pour évaluer la sécurité de nos systèmes et les connaissances de nos collaborateurs seront désormais conduits régulièrement.
6. Un **courrier d'information** sera adressé d'ici quelques jours aux citoyens.

« Unie, la Municipalité partage le désarroi de ses citoyens par rapport à cette attaque dont l'ampleur est sans précédent, autant pour eux que pour notre Commune. Elle s'engage à faire tout ce qui est en son pouvoir pour surmonter cette épreuve et à communiquer aussi souvent que nécessaire les informations pertinentes en sa possession. Elle met tout en œuvre afin de pouvoir adresser des réponses personnalisées dans un avenir proche. » déclare Monique Pugnale, syndique de Rolle, au nom de la Municipalité.

Contact : Voxia communication – philippe.cathelaz@voxia.ch

