ROLLE
PERLE du LÉMAN

COMMUNIQUÉ DE PRESSE

CYBERATTAQUE CONTRE L'ADMINISTRATION ROLLOISE – MESSAGE DE LA MUNICIPALITÉ – INFORMATIONS DE SUIVI SUR LE TRAVAIL D'ANALYSES DES DONNÉES

Rolle, le 3 septembre 2021 – **À la suite de la cyberattaque dont elle a été victime, la Commune de Rolle a entrepris l'important travail d'analyse des données disponibles sur le darkweb. Elle ouvre ici un journal d'informations qui sera complété au fur et à mesure. Avec l'aide du Canton, la procédure d'analyse a été établie en concertation avec l'Autorité de Protection des données et du droit à l'information. Un courrier a été envoyé à la population et un risque de fraude a été empêché.**

Dimanche 29 août – Appel à la vigilance

Par voie de communiqué de presse, la Municipalité a donné un premier état des lieux des travaux de la task force, apporté des détails sur la chronologie des faits et appelé la population à la vigilance.

Lundi 30 août – Procédure d'analyse des données validée

La task force a rencontré la Préposée cantonale à la Protection des données (APDI). Cette séance de travail a permis de finaliser et d'adopter une méthodologie pour classifier les informations consultées selon 4 niveaux de sensibilité et la procédure d'analyse qui distingue notamment deux étapes : opérationnelle (classification de l'ensemble des documents) et décisionnelle (quelle suite donner aux informations en fonction de leur niveau de sensibilité).

Chaque boîte email doit être analysée par deux personnes, dont le collaborateur concerné. Cette approche rigoureuse d'analyse se conforme aux exigences de la loi sur la protection des données personnelles (LPrD) ; elle demande du temps et se distingue en cela des méthodes utilisées par celles et ceux qui consulteraient ces données sur le darkweb.

Le Canton de Vaud et l'APDI ont délégué avec effet immédiat des ressources et des expertises pour aider la Commune de Rolle dans ce travail colossal. La task force se réunit chaque jour et la Municipalité assure un contact journalier avec le Canton.

Mardi 31 août – Envoi d'un courrier aux ménages et création d'une page web dédiée

Un courrier d'information a été envoyé à chaque ménage et chaque entreprise de la Commune de Rolle. Ce message d'information à la population est l'une des mesures qui lui sont destinées pour l'aider à comprendre l'enchaînement des faits et à augmenter sa vigilance.

Le site web de la Commune a désormais une page dédiée à la cyberattaque. On y retrouve les informations diffusées à la presse et les news qui rendent compte du travail de la taskforce. Cette section accueillera prochainement des informations utiles en matière de cybersécurité ainsi qu'un formulaire sécurisé pour déposer des demandes précises et personnelles au sujet de la cyberattaque.

Mercredi 1er septembre – Un risque de fraude avec 30 bons d'achat émis par la Commune de Rolle a été empêché

Des bons d'achat émis par la Commune pour soutenir les entreprises rolloises durant la période Covid ont été identifiés dans une boîte mail disponible sur le darkweb.

Après vérification, 30 de ces bons présentaient un solde encore ouvert, engendrant un potentiel risque de fraude. Ceux-ci ont été immédiatement désactivés. La Municipalité a pris contact directement avec les détenteurs de ces bons pour les informer de cette situation et leur proposer de nouveaux bons affichant un solde identique. Cette option a été privilégiée afin de ne pas bloquer la totalité des bons et de permettre aux citoyens et commerçants de continuer à profiter de l'offre.

Pour rappel, les utilisateurs reçoivent une confirmation par email à chaque usage de leur bon, ce qui permet de détecter des fraudes éventuelles. À ce jour, aucune anomalie n'a été signalée. La Municipalité invite la population à l'informer en cas de problème rencontré avec un bon.

Mercredi 1er septembre – Mention dans la presse d'un rapport d'audit

La presse mentionne un audit informatique commandité par la Commune de Rolle. Cet audit a été planifié à l'initiative de la Commune et le rapport est daté du 11 mai, soit quelques jours avant l'attaque. Il fait l'objet d'un plan de remédiation interne. De plus, comme annoncé le 25 août, la Municipalité conduira régulièrement des audits de cybersécurité.

Jeudi 2 et vendredi 3 septembre – État des lieux

Poursuite du travail d'analyse des 4'000 fichiers et des boîtes mail.

Au sujet de la demande de rançon

Le rançongiciel a permis aux cybercriminels de chiffrer l'ensemble des données sur les serveurs informatiques de la Commune. La demande de prise de contact est apparue le 30 mai sur les écrans des ordinateurs lorsque l'accès aux données et emails s'est avéré impossible. Alignée sur les recommandations des experts impliqués et du Centre national pour la cybersécurité, la Municipalité n'est pas entrée en matière.

https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html

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