Ville de
Joinville-le-Pont

Note d'information relative à un incident de sécurité informatique

La commune de Joinville-le-Pont a identifié une intrusion informatique visant l'un des logiciels métiers de la Police Municipale. Cette attaque a entrainé un accès non autorisé et l'exfiltration des données qu'il contient.

Le logiciel concerné est celui utilisé par la Police Municipale de la commune pour la gestion des registres d'accueil, du CSU et des mains courantes, des stationnements gênants, des mises en fourrières, des opérations tranquillité vacances et des procès-verbaux.

Quelles sont les données concernées ?

Il résulte des investigations que l'exfiltration concerne uniquement les données saisies à partir du 19 mars 2024. Les données saisies avant cette date n'ont pas été impactées.

Au total, les informations personnelles d'environ 10.000 personnes (requérants, mis en causes, témoins, victimes, propriétaire) ont été extraites. Les données varient selon le type de dossier :

- mains courantes (données d'identité, coordonnées, rôle, date et description des faits ainsi que toute information renseignée dans le cadre de la main courante) ;
- procès-verbaux, mis en
- cause (données d'identité, coordonnées, détails concernant les infractions et toute information renseignée dans le cadre du procès-verbal) ;
- registre d'accueil (données d'identité, coordonnées, rôle, date et description des faits ainsi que toute information renseignée dans le registre d'accueil)
- registre CSU (données d'identité, coordonnées, rôle, date et description des faits ainsi que toute information renseignée dans le registre CSU)
- dossiers d'Opérations Tranquillité Vacances (données d'identité, coordonnées, périodes d'absence du domicile) ;
- dossiers de stationnement gênant (données d'identité, coordonnées, informations sur les véhicules) ;
- dossiers de fourrière (données d'identité, coordonnées, informations sur les véhicules).

Sous réserve des restrictions mises en œuvre pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour protéger la sécurité publique ou pour protéger les droits et libertés d'autrui, la commune a pris contact individuellement avec chaque personne concernée dès lors que ses coordonnées téléphoniques avaient été communiquées.

Quels sont les risques identifiés pour les personnes concernées ?

Les données extraites du logiciel ont été publiées sur un forum cybercriminel. Les risques que nous identifions à partir des informations extraites sont les suivants :

- Escroquerie et Phishing : Tentatives d'escroquerie par SMS ou téléphone, notamment par des individus se faisant passer pour les services de police ou l'administration ;
- Usurpation d'identité ;
- Représailles ou harcèlement : Risque lié à la divulgation de l'identité d'un requérant auprès d'un mis en cause ;

- Cambriolages : Risque ciblant les domiciles dont les dates d'absence ont été compromises dans le cadre des opérations tranquillité vacances.

Quelles mesures ont été prises ?

Dès constatation de l'exfiltration des données, l'accès à la plateforme a été sécurisé et des investigations ont été réalisées pour évaluer le périmètre des données concernées.

Conformément à ses obligations en matière de protection des données personnelles, la commune a notifié la violation de données à la Commission nationale de l'informatique et des libertés (Cnil).

Une plainte pénale a également été déposée et la commune est en contact avec l'ANSSI (Agence nationale de la sécurité des systèmes d'information) afin de bénéficier de leur accompagnement technique et de coordonner les actions de sécurisation avec l'Urgence Cyber Île-de-France.

Les actions de remédiation qui ont été mises en œuvre par la commune sont les suivantes :

- Désactivation immédiate du compte utilisateur compromis ayant permis à l'attaquant d'extraire les données ;
- Sécurisation globale : réinitialisation forcée et obligatoire des mots de passe de l'ensemble des personnels de la collectivité habilités à se connecter au logiciel métier concerné ;
- Audit de sécurité visant l'intégralité des journaux de connexions de tous les agents de la Police Municipale permettant de confirmer l'absence d'autre compte compromis ;
- Suppression des droits d'extraction et d'exportation sur l'ensemble des modules sensibles (mains courantes, procès-verbaux, opérations tranquillité vacances, stationnement, fourrière) ;
- Coupure des accès aux outils critiques d'administration, de supervision, de consultation des journaux d'activité du logiciel rendant techniquement impossible tout nouvel export de masse.

Nos recommandations

Il est recommandé de faire preuve de la plus grande vigilance face au risque de SMS ou appels frauduleux. En cas de suspicion ou de situation anormale, il est recommandé de contacter le service officiel d'assistance aux victimes numériques www.cybermalveillance.gouv.fr pour effectuer un signalement et faire valoir vos droits.

En cas de pressions, de harcèlement ou de tout comportement suspect lié à cet incident, nous vous invitons à prendre contact avec les autorités judiciaires compétentes.

La commune exprime ses plus sincères regrets pour cet incident et tient à assurer les usagers de son engagement total pour en minimiser les conséquences. La transparence, la responsabilité et la sécurité demeurent nos priorités absolues.

Contact

La commune se tient à votre disposition pour vous assister dans vos démarches. Pour toute question complémentaire, vous pouvez contacter notre Délégué à la Protection des Données (DPO) à l'adresse email suivante : dpd@joinvillelepont.fr.

Par ailleurs, les services de la Police Municipale demeurent pleinement opérationnels :

- Les patrouilles de terrain ainsi que les interventions quotidiennes sont maintenues normalement.
- L'accueil du public au sein du poste de police reste ouvert aux horaires habituels.
- Les numéros d'appel d'urgence de la Police Municipale fonctionnent parfaitement.

Certaines démarches administratives internes peuvent toutefois connaître de légers ralentissements temporaires.