CACG
Valorisons votre territoire

le 15 décembre 2023

Madame, Monsieur, chers clients, fournisseurs, prestataires et partenaires

La CACG a subi samedi 9 décembre une attaque informatique, impactant l'ensemble de notre système d'informations.

Depuis cette date, l'équipe informatique et le Comité de Direction se sont mobilisés avec une très grande réactivité et sont accompagnés par une équipe d'experts spécialisés en matière de cybersécurité afin de sécuriser notre système informatique et restaurer progressivement les premières fonctionnalités, tout en menant l'ensemble des investigations liées à l'attaque.

Conformément aux obligations légales et réglementaires nous avons porté plainte auprès des autorités compétentes et un signalement a été réalisé auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés).

A ce jour, nous n'avons pas de date de retour à la normale.

Compte tenu de la typologie de l'attaque subie, l'exfiltration de données personnelles doit être anticipée. Les risques de réutilisation de vos données personnelles ne peuvent être totalement exclus.

Nos investigations sont en cours pour connaître plus précisément l'ampleur et la nature d'une exfiltration éventuelle.

Par mesure de prudence, nous vous conseillons de suivre les recommandations suivantes :

- Surveiller les courriels que vous recevrez via votre adresse mail afin de ne pas faire l'objet de campagne de spam électronique ou d'hameçonnage.
- Vous montrer vigilant à l'égard des messages de source douteuse, qui vous inviteraient à préciser des informations personnelles ou des données d'identification, à ouvrir une pièce jointe ou encore à cliquer sur un lien vers un site internet.
- Ne jamais communiquer de données sensibles vous concernant par mail ou par téléphone.
- Bien contrôler, dans les prochains mois, vos relevés bancaires notamment quant à la présence de tout prélèvement, même de faible montant et de contacter votre banque afin de mettre éventuellement en place une surveillance spécifique en cas de mouvement anormal sur votre compte bancaire.
- Modifier l'ensemble de vos mots de passe et utiliser un mot de passe unique et complexe.
- Prévenir les organismes concernés tels que la CPAM, les Finances publiques, la CAF etc. Il est conseillé de surveiller les mouvements liés à ces comptes afin d'identifier des prélèvements anormaux.

CACG
Valorisons votre territoire

le 15 décembre 2023

Pour aller plus loin :

- Vérifier la légitimité d'un mail reçu, puis de signaler les mails suspicieux sur cette cybermalveillance.gouv.fr.
- Vérifier ou signaler, sur cette plateforme les sites internet suspicieux.
- Mettre en place une double authentification pour sécuriser les accès aux sites et applications.

Lorsque des informations bancaires et/ou des identifiants bancaires ont été impactés :

- Contacter votre banque afin de mettre en place une surveillance spécifique et ainsi prévenir tout mouvement anormal sur votre compte bancaire (établissement d'une « liste blanche » des créanciers spécifiquement autorisés à prélever sur votre compte - tout prélèvement émis par un créancier absent de cette liste sera rejeté, autorisation de règlement par SMS ou sur le site de votre banque via un mot de passe).
- Bien contrôler, dans les prochains mois, vos relevés bancaires notamment quant à la présence de tout prélèvement, même de faible montant.
- Modifier immédiatement vos mots de passe et code de sécurité.

Si vous pensez être victime d'une usurpation d'identité : obtenir des conseils sur les mesures à prendre en cas d'usurpation d'identité sur le site cybermalveillance.gouv.fr et/ou sur la page dédiée préparée par la CNIL et/ou **contacter le service téléphonique d'information de la police nationale Info-escroqueries** au 08 11 02 02 17 (prix d'un appel local), et déposer plainte au plus vite auprès d'un commissariat de police ou de gendarmerie.
Si l'usurpation est confirmée, vous pouvez demander auprès des services de la CNIL une consultation du fichier des comptes bancaires (FICOBA) afin de savoir si des comptes ont été ouverts à votre nom par l'escroc.

En cas de questions complémentaires, nous vous invitons à adresser toute sollicitation éventuelle vers l'adresse **dpo.cacg@gmail.com** ou par téléphone au **05 62 51 71 49.**

La présente communication intervient dans le respect des articles 33 et 34 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

Espérant retrouver au plus vite un fonctionnement normal pour notre entreprise, je tiens à remercier chacun d'entre vous pour l'élan de solidarité auquel nous assistons depuis le début de la semaine.

Willy LUIS,
Directeur Général