COMMUNE DE
Strassen

AVIS AU PUBLIC

Mesdames, Messieurs,

Nous avons le regret de vous informer que la Commune, et notamment le service technique (département de l'urbanisme – service des autorisations de bâtir) de la Commune de Strassen a fait l'objet d'une attaque de type Malspam le 7 février 2025, entrainant une violation de données à caractère personnel au sens de l'article 33 du RGPD.

Dès que nous nous sommes aperçus de cette attaque, notre équipe IT a immédiatement déconnecté du réseau l'ordinateur compromis et pris toutes les mesures nécessaires pour qu'une telle attaque ne puisse se reproduire.

Quel type d'attaque ?

Ce type d'attaque cible les organismes via des e-mails frauduleux exploitant des outils de gestion et de surveillance à distance (Remote Monitoring & Management – RMM).
Les attaquants profitent de l'attaque pour tromper les destinataires en les faisant cliquer sur un lien malveillant, déguisé en facture, qui installe un outil RMM sur leur système. Comme ces outils sont des applications légitimes, ils contournent les antivirus et permettent aux attaquants d'obtenir un accès distant complet.
Les attaquants sont susceptibles d'avoir installé des outils RMM supplémentaires en diffusant des e-mails malveillants via nos carnets d'adresses électroniques.
L'objectif principal de ces attaques est d'exploiter les stations de travail compromises – souvent celles des comptables ou responsables financiers – pour **intercepter les codes PIN des cartes à puce** et exécuter des **transferts frauduleux**, entraînant des pertes financières.

Quels risques encourez-vous ?

Si vous avez déposé une demande d'autorisation de bâtir ou figurez comme contact dans nos carnets d'adresses électroniques, vous êtes susceptibles d'avoir fait ou de faire l'objet d'une telle attaque et, en cliquant sur le lien malveillant déguisé en facture, de donner ainsi accès distant complet sur votre ordinateur aux attaquants, y compris à vos instruments financiers et à votre carnet d'adresses.

Quelles sont les mesures de précaution à prendre?

En premier lieu : ne cliquez pas sur une pièce jointe provenant de la Commune ou autre sans vérifier au préalable au téléphone qu'elle est sûre.

- Ne pas cliquer sur des liens suspects.
- Survol des liens avant de cliquer pour vérifier leur destination.

Que faire en cas de compromission ?

Si vous pensez avoir fait l'objet d'une attaque :

- Déconnecter immédiatement l'ordinateur compromis du réseau (y compris le Wi-Fi !).
- Vérifiez vos instruments financiers.
- Identifier d'autres systèmes potentiellement touchés.
- Avertir vos contacts de ne pas ouvrir de liens provenant de votre adresse e-mail.
- Soyez vigilant à l'égard des pièces jointes.
- Réinstaller totalement le système affecté (un simple scan antivirus ne suffit pas)
- Consultez un professionnel IT
- Changez tous vos mots de passe.

Pour toute question relative à cette violation de données, vous pouvez contacter notre service technique au 31 02 62 - 300 et/ou notre délégué à la protection des données, la société ProNewTech S.A. à l'adresse e-mail suivante : dpo@strassen.lu.

Nous sommes sincèrement navrés de cette violation. Votre vie privée est notre priorité et nous continuerons à surveiller la situation et à utiliser tous les recours possibles pour protéger vos données personnelles. Merci pour votre confiance.

Strassen, le 7 mars 2025
(s) le Collège échevinal