Le SICTAME vous informe

www.sictame-unsa-total.org

Informatique et libertés des salariés

Le logiciel « KeePass » a été installé mi-décembre 2017 sur votre ordinateur. Il s'agit d'un logiciel d'utilisation libre qui permet de gérer et de sauvegarder des mots de passe dans une « base de données » chiffrée, accessible grâce à un mot de passe principal.

Ce qui interpelle le SICTAME, c'est que la direction *suggère* aux salariés de l'utiliser pour sauvegarder leurs mots de passe *personnels* *(bancaires, messageries, dossier médicaux, réseaux sociaux, …)* et que le dossier concernant ces mots de passe soit sauvegardé sur le disque dur de l'ordinateur professionnel du salarié.

Selon l'Intranet[1] :

> With KeePass it is possible to create multiple databases that hold the account information, for example you could have a database for your Total work passwords and ***one for your personal passwords.*** It is strongly recommend you separate your work and personal password information.
>
> Please check with the provider of any personal sites or services, ***such as your bank,*** that they support the use of Password wallets prior to using KeePass.

Le SICTAME prend très au sérieux la protection des données privées des salariés

Le SICTAME a posé un certain nombre de questions à la direction sur le KeePass et demandé une réunion avec l'équipe en charge du dossier afin de s'assurer de l'absence de risques pour ces données personnelles si sensibles.

La direction a refusé de répondre positivement à cette demande. Par contre, elle a fait une déclaration très intéressante : « *ces dossiers sont cryptés, et il serait impossible d'y accéder, absolument aucun risque pour les salariés !* »

Le SICTAME souhaite cependant attirer l'attention des salariés sur certains points

- La direction rechigne à donner les raisons qui l'ont amenée à suggérer le stockage des mots de passe privés sur les disques durs ;
- Les prestataires informatiques (dont certains localisés en Inde) ont la possibilité d'accéder aux disques durs des salariés et donc, théoriquement, à ces dossiers KeePass contenant vos mots de passe. Bien sûr, il faudrait ensuite les décrypter. Mais est-ce vraiment impossible ?
- Dire que le logiciel KeePass est invulnérable n'engage que la direction et il suffit de rechercher « KeePass » ou « KeePass vulnerabilities » sur Internet pour avoir beaucoup de doutes sur ce « mythe » ;

[1] http://wat.corp.local/sites/s361/en-US/Pages/KeePass.aspx

- Le SICTAME est particulièrement choqué du fait que la direction recommande aux salariés la sauvegarde de leurs précieux dossiers personnels dans les ordinateurs de la société.
- **Le SICTAME déconseille aux salariés d'utiliser KeePass pour sauvegarder leurs mots de passe personnels dans leurs ordinateurs professionnels, ainsi que d'utiliser ces ordinateurs pour accéder à des informations d'ordre privé.**

Pour améliorer la protection de vos mots de passe

Le SICTAME recommande de télécharger KeePass chez vous, sur vos ordinateurs personnels, et de ne jamais utiliser le clavier des ordinateurs professionnels pour vos mots de passe privés, de sauvegarder ensuite ce fichier sur une clé USB sécurisée (par exemple avec une clef USB à petit clavier mot de passe incorporé, tel que le recommande d'ailleurs la sécurité informatique du Groupe dans l'Intranet pour protéger les fichiers professionnels pendant les déplacements).

Ce n'est pas la première fois que la direction agit curieusement en matière de protection de données personnelles des salariés. Souvenons-vous en effet de Zscaler, solution utilisée par le Groupe qui, à l'insu des salariés, « casse » le SSL[2] entre le site Intranet consulté et l'ordinateur professionnel (c'est là qu'apparaît la petite fenêtre ci-dessus). Ceci pourrait ouvrir la porte d'accès à vos données personnelles et à vos mots de passe.

La loi Informatique et Libertés est en cours de révision afin de la mettre en conformité avec les nouvelles règles européennes avant le 25 mai 2018. La protection des données des salariés sera renforcée et les manquements lourdement sanctionnés - jusqu'à 4 % du chiffre d'affaires. Le salarié pourra demander la copie intégrale de ses données et pourra s'opposer à toute utilisation de ses données qui ne serait pas liée à son contrat de travail ou à sa carrière, par exemple pour l'évaluation de ses performances.

Enfin, le SICTAME s'étonne que la direction ait retiré à des salariés informaticiens du Groupe des mots de passe " administrateur " nécessaires à leur travail pour les donner à des prestataires situés en Inde ! Ces droits d'administrateurs leur permettent de se promener presque partout dans nos serveurs et parmi nos données, professionnelles ou non. Cette mesure, décidée certainement dans le but d'une réduction de coûts, est-elle une vraie bonne idée ? La sécurité des données Groupe, si chère à la direction, peut-elle être assurée dans ces conditions ?

Pour toute question concernant la protection de vos données personnelles dans l'entreprise, contactez le SICTAME

SICTAME UNSA

Suivez nous sur
http://www.sictame-unsa-total.org/fr
https://twitter.com/sictame
Souscrivez également à notre **bulletin électronique**
en écrivant à
holding-amont.sictame-unsa-ues@total.com

SICTAME-UNSA-TOTAL

- Tour Coupole La Défense Bureau 4E41 (01.47.44.76.33)
- Pau Bureau F16 CSTJF (05.59.83.64.83)
- Michelet La Défense Bureau B RD 09 (01.41.35.75.93)
- Spazio Nanterre Bureau A10036 (01.41.35.34.48)

[2] ***Secure Sockets Layer*** (**SSL**), protocole de sécurisation des échanges sur Internet.