Télétravail : la Cnil donne une prime à Tixeo et à l'authentification forte

L'authentification forte ? Il faut la généraliser dans la mesure du possible.

La Cnil en a fait l'un des leitmotive d'un guide destiné à accompagner la mise en œuvre du télétravail.

Ledit guide, publié sous licence GPLv3, est ouvert aux contributions. Il s'organise en deux sections principales regroupant respectivement des conseils à l'adresse des particuliers et des entreprises.

Pour ces dernières, allusion est faite à l'authentification forte – plus précisément à double facteur – pour la protection des VPN et des services accessibles à distance.

La Cnil conseille par ailleurs de privilégier, pour la communication, les logiciels qui assurent un chiffrement de bout en bout.

C'est le cas de Tixeo, édité par la société montpelliéraine du même nom et que la commission suggère au rang des « systèmes de visioconférence qui protègent la vie privée ».

La recommandation porte plus précisément sur l'édition TixeoServer, dont le client assure l'exploitation. L'Anssi lui a accordé une certification de premier niveau qui en permet notamment l'utilisation par les OIV et les administrations.

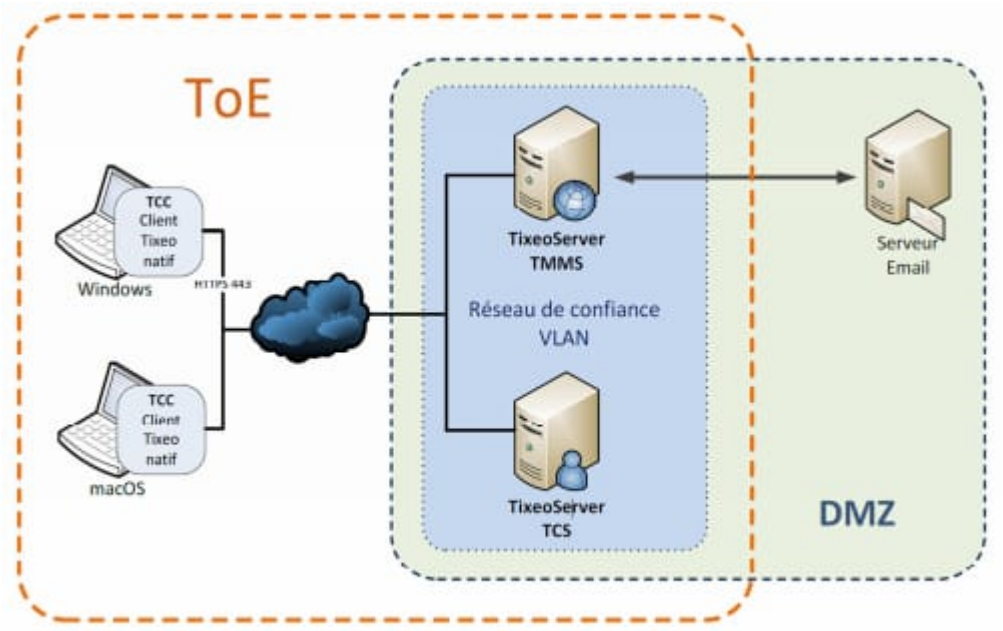

Figure 1 - Architecture de la solution TixeoServer.

Sécurité : on n'oublie pas sa box

Malgré les garanties qu'il offre en matière de sécurité et de confidentialité, l'usage de Tixeo devra, insiste la Cnil, s'assortir de bonnes pratiques. Entre autes, désactiver l'enregistrement des mots de

passe par les navigateurs web.

Parmi les autres conseils que fournit ce « guide télétravail », on aura relevé, pour les entreprises :

- L'édition d'une charte de sécurité ou au moins d'un socle de règles minimales à respecter
- Sur les postes de travail, la mise en place, *a minima*, d'un pare-feu, d'un antivirus et d'un blocage de l'accès aux sites malveillants
- L'application régulière, aux équipements et aux logiciels, des derniers correctifs de sécurité
- La consultation régulière des journaux d'accès des services accessibles à distance

Et pour les particuliers :

- S'assurer du bon paramétrage de sa box Internet (mot de passe administrateur, logiciel interne, sécurité du Wi-Fi)
- Privilégier l'utilisation des ressources connectées au VPN et ne désactiver ce dernier que lorsqu'on utilise des services consommateurs en bande passante
- Être vigilant sur les tentatives d'hameçonnage

À consulter en complément :

- Un guide de la sécurité des données personnelles
- Une précédente liste de bonnes pratiques pour les salariés en télétravail
- Le guide d'hygiène informatique de l'Anssi

Photo d'illustration via *Pixabay*