

# L'App Outlook interdite au Parlement Européen

Quelques jours seulement après le lancement par Microsoft de la nouvelle App Outlook pour iOS et Android, la DG ITEC (DSI du Parlement européen) vient d'en interdire l'usage à tous les membres du Parlement européen. Motif invoqué : L'application pose d'importants problèmes de sécurité. Ainsi, la DG ITEC a adressé en interne à l'ensemble des utilisateurs le message suivant : *« Vous êtes priés de ne pas installer ces applications, et au cas où vous les auriez déjà installée pour accéder à votre messagerie professionnelle, nous vous demandons de les désinstaller immédiatement et de changer votre mot de passe [...] les applications envoient sans permission des informations de mot de passe à Microsoft et stockent les courriels dans un service cloud de tierce partie sur lequel le Parlement n'a aucun contrôle. »* Microsoft a officiellement réagit ce matin (15 février) en annonçant travailler avec les administrateurs du Parlement européen afin de fournir la documentation nécessaire pour éviter les comportements dangereux de l'application. Microsoft a également reconnu travailler sur l'amélioration de la sécurité de l'application et s'est engagé à une mise à jour dans les prochains mois.

On ne peut que se réjouir de la vigilance de la DSI du Parlement Européen sur cette affaire mais s'interroger quand même sur la réactivité de nos institutions sur d'autres incidents de sécurité. Puisque nous parlons d'Outlook sous iOS, pourquoi par exemple une vulnérabilité critique découverte dans iOS le 8 janvier 2014 et corrigée par Apple le 21 février 2014 n'a-t-elle fait l'objet d'aucun message d'alerte de la part de l'ENISA ou de l'ANSSI ? Certes le bulletin Bulletin d'actualité (CERTFR-2014-ACT-009) de l'ANSSI l'indique effectivement le 28 février 2014 mais le risque réel se situait entre le 8 janvier (première exploitation effective de la faille) et le 21 février (disponibilité du correctif fourni Apple). Et dans cet exemple, ce n'est pas uniquement les mots de passe de messagerie qui pouvaient être compromis par une attaque MITM totalement transparente mais l'ensemble des flux chiffrés entre le terminal (iPhone ou iPad) et le Cloud (mots de passe de toutes les applications, numéros de cartes bancaires, etc...).

---

Autres ressources :

- Le Parlement européen bannit les apps Outlook pour iOS et Android
- La nouvelle application Outlook interdite au Parlement européen
- Microsoft Working with European Parliament to Unban Outlook Android/iOS App