Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGÉRENCE ÉCONOMIQUE

Flash n° 39 – Janvier 2018

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°39 Janvier 2018

Les vulnérabilités liées à l'utilisation professionnelle des smartphones

Des cas de compromission ou de captation informationnelle liés à l'utilisation de smartphones dans un cadre professionnel sont régulièrement observés. Ils surviennent bien souvent à l'occasion de déplacements à l'étranger ou, plus communément, à la suite d'un usage non sécurisé.

1er exemple

Lors d'un congrès professionnel, les participants ont pu télécharger directement sur leur smartphone une application qui leur permettait, grâce à la géolocalisation, de localiser dans un rayon défini les autres congressistes ou de rechercher l'un d'entre eux en particulier.

Les conditions d'utilisation de cette application indiquent, entre autres, que dans les pays où le programme est utilisé, les données des utilisateurs pourront être communiquées aux autorités qui en feraient la demande. Par ailleurs, en cas de vente des actifs du groupe, toutes ces informations seront cédées à l'acquéreur.

Les fonctionnalités de l'application (GPS, Wi-Fi, stockage de données sur un serveur extérieur, etc.) soulèvent des questions de confidentialité des échanges entre congressistes. Des interrogations se posent également sur la conservation et, le cas échéant, l'utilisation des informations personnelles et professionnelles téléchargées via cette application.

2ème exemple

Certaines marques de téléphones mobiles utiliseraient des applications système préinstallées afin de transmettre, à des sociétés extra-européennes notamment, des données collectées sur les smartphones, à l'insu de l'utilisateur et de manière non chiffrée.

Les entreprises se défendent en arguant qu'il ne s'agit que de données techniques, mais compte tenu qu'il est possible d'identifier un client grâce aux informations de son smartphone, il s'agit d'une vulnérabilité qu'il convient de ne pas négliger.

3ème exemple

À l'occasion d'un salon professionnel, un industriel extra-européen proposait à ses clients de scanner des codes 2D tels que les codes QR, afin d'avoir plus d'informations sur l'entreprise et ses produits.

Le client était invité à accéder au site avec son smartphone pour obtenir la documentation, qu'il ne trouvait cependant pas.

Cette opération permettait en revanche à l'industriel de récupérer des informations figurant sur le téléphone mobile utilisé pour scanner le code.

Commentaires

L'utilisation des smartphones est très largement répandue dans l'environnement professionnel.

Ils permettent de consulter les courriels professionnels, de naviguer sur Internet ou encore de se connecter sur des réseaux d'entreprise pour travailler, comme il serait possible de le faire depuis un poste fixe de travail.

En outre, de nombreux utilisateurs ont un usage dual de leur téléphone professionnel, l'utilisant également à des fins personnelles pour télécharger, notamment, des applications ludiques ou un accès aux différents réseaux sociaux.

Comme le souligne l'ANSSI[1] (Agence nationale de la sécurité des systèmes d'information), il est illusoire d'espérer atteindre un haut niveau de sécurité avec un smartphone, quel que soit le soin consacré à son paramétrage. Il est toutefois nécessaire de protéger au mieux les données qu'il contient.

Préconisations de la DGSI

Afin de limiter les risques de compromission ou de captation informationnelle liés à l'usage professionnel des smartphones, la DGSI émet les préconisations suivantes :

Risque de vol :

- Protéger les données contenues dans le smartphone par un verrouillage systématique de l'écran.
- Verrouiller son téléphone portable par un code alphanumérique de 8 caractères.
- Chiffrer les données sensibles grâce à des solutions de chiffrement pour smartphones.

[1] Note technique « *Recommandations de sécurité relatives aux ordiphones* », 28/07/2015.

- Prévenir la DGSI en cas de vol ou de perte d'un téléphone professionnel pouvant contenir ou contenant des informations sensibles ou stratégiques.

Vulnérabilité du système :

- Mettre à jour régulièrement le système d'exploitation et l'ensemble des applications téléchargées sur le smartphone.

- Afin de se protéger contre l'installation d'une application malveillante, ne jamais cliquer sur un lien d'origine inconnue et éviter de scanner des QR codes.

- Avant de télécharger une application, vérifier sa provenance et ses droits d'accès aux données du téléphone.

- S'assurer du téléchargement des applications et de leur mise à jour à partir d'une plateforme officielle.

- Rester vigilant aux potentielles atteintes à la confidentialité liées à l'accès aux données personnelles.

Géolocalisation :

- Désactiver systématiquement la fonction géolocalisation une fois utilisée.

- Les photos et vidéos indiquent par ailleurs le lieu, la date et l'heure de la prise de vue dans les métadonnées.

Wi-Fi[2] :

- Installer un VPN (*Virtual Private Network*) permettant la transmission chiffrée des données. Certains VPN sont directement téléchargeables sur les smartphones via des applications.

- Ne pas laisser le Wi-Fi actif sans nécessité, celui-ci transmettant en permanence l'historique et la géolocalisation de vos anciennes connexions.

[2] Cf. FI N°23 AVRIL 2016 – Les dangers liés aux Wi-Fi publics.

Bluetooth :

- Désactiver la fonction après utilisation.

Utilisation :

- Limiter le plus possible l'utilisation du smartphone professionnel à des fins personnelles et inversement.

- Dans le cadre d'un déplacement professionnel à l'étranger, privilégier l'utilisation d'un téléphone dédié et, le cas échéant, l'emploi d'une pochette de type « cage de Faraday » avant d'accéder à des locaux sensibles.

Recommandation générale :

- Consulter sur le site de l'ANSSI la note technique « *Recommandations de sécurité relatives aux ordiphones* », qui émet 21 recommandations afin de sécuriser au mieux l'emploi de téléphones portables en environnement professionnel.