Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 55 – Septembre 2019

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°55 Septembre 2019

Les risques liés à l'utilisation des réseaux WiFi publics

Depuis plusieurs années, l'utilisation d'appareils électroniques nomades pouvant se connecter à Internet connait une croissance exponentielle. En effet, tant pour un usage personnel que professionnel, de plus en plus de personnes se connectent directement sur leur téléphone ou leur ordinateur portables à Internet, souvent par le biais de réseaux WiFi publics.

Ces réseaux sont toutefois souvent vulnérables et peuvent être piratés par des individus malveillants, notamment dans un but de captation d'informations sensibles.

PREMIER EXEMPLE

Un groupe d'attaquants a ciblé plusieurs hôtels de luxe dans le but d'infecter leur réseau wifi. Grâce à des courriels piégés, les attaquants auraient réussi à installer un maliciel afin de se latéraliser et de compromettre les réseaux wifi des établissements visés. Une telle opération leur aurait permis de récupérer les identifiants et mots de passe des clients de ces hôtels sur leurs propres wifi.

DEUXIEME EXEMPLE

Un dirigeant d'entreprise française en déplacement éclair dans un pays extra-européen s'est connecté avec son ordinateur professionnel à plusieurs réseaux wifi (hôtel, aéroport, restaurants, etc.) afin d'envoyer des courriels sensibles relatifs à un appel d'offre. Or, suite à ces envois, le concurrent du groupe français, proche des autorités du pays étranger, semble s'être immédiatement aligné sur l'offre tricolore, remportant ainsi *in extremis* le marché en question.

Bien qu'il soit impossible de prouver l'implication des autorités du pays étranger dans l'opération, elles pourraient avoir profité du séjour du dirigeant français, et notamment de ses connexions sur des réseaux publics non sécurisés, pour recueillir un maximum d'informations sur l'appel d'offre en cours.

COMMENTAIRES

Aujourd'hui, la plupart des lieux publics (restaurants, cafés, aéroports, hôtels, centres commerciaux, gares, etc.) en France et à l'étranger, proposent à leurs clients ou aux simples visiteurs un accès gratuit à Internet via des réseaux Wi-Fi.

Dans le cadre de déplacements professionnels mais également personnels, il est alors tentant d'y connecter son smartphone, sa tablette ou son ordinateur portable afin d'accéder à diverses ressources informatiques (messageries électroniques, compte bancaire, réseaux sociaux, extranet, espace de stockage en ligne, etc.).

Ces accès publics sont néanmoins généralement vulnérables, en raison d'un faible niveau de sécurité. Des utilisateurs malveillants peuvent notamment exploiter ces failles pour intercepter les communications (identifiants de connexion à des messageries électroniques, mots de passe, numéro de carte bancaire, historique de navigation Internet, etc.) transitant par ces points d'accès Wi-Fi.

Il est également très facile pour des pirates informatiques de créer de vrais-faux réseaux Wi-Fi usurpant le nom d'une enseigne reconnue, accessibles gratuitement et sans mot de passe. Cette manœuvre leur permet de récupérer des informations techniques sur les systèmes, ainsi que de nombreuses données personnelles et sensibles facilitant de nouvelles intrusions informatiques.

PRECONISATIONS DE LA DGSI

Afin de réduire les risques de vol de données sensibles d'une connexion à un Wi-Fi public, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

→ Utiliser obligatoirement un VPN en cas d'utilisation d'un point d'accès Wi-Fi public.

→ Utiliser de préférence des messageries mail chiffrées pour échanger des contenus sensibles.

→ Sécuriser ses données et ses échanges en utilisant un outil de chiffrement, type PGP, disponible en téléchargement libre.

→ Désactiver le mode Wi-Fi quand il n'est pas utilisé.

→ Mettre à jour régulièrement le système d'exploitation, le navigateur Internet (et ses extensions), son antivirus et les logiciels comme Adobe Reader et Flash.

→ Privilégier les sites Internet sécurisés utilisant du HTTPS (une extension à installer sur les navigateurs Internet telle que HTTPSANYWHERE permet également d'automatiser le passage de certains sites Internet en HTTPS).

→ En cas de doute après avoir été connecté à un WiFi public, changer rapidement les mots de passe des applications (messageries électroniques, réseaux sociaux, comptes bancaires, espace de stockage en ligne, etc.) que vous utilisez le plus souvent.

→ En cas de déplacement, privilégier l'utilisation d'appareils nomades vierges chiffrés dédiés exclusivement aux voyages.

→ Faire remonter au directeur sécurité de son entreprise ainsi qu'à la DGSI tout problème constaté.

→ Consulter sur le site de l'ANSSI la note technique « *Recommandations de sécurité relatives aux réseaux WiFi* ».