Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 25 - Juin 2016

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° 25 Juin 2016

Les dangers liés aux objets connectés

L'engouement massif pour les objets connectés ne se limite pas seulement au grand public. Le phénomène concerne également de plus en plus les entreprises.

Qu'il s'agisse d'équipements personnels (bracelets, montres, cigarettes électroniques, etc.) apportés et utilisés au sein des locaux de l'entreprise par les salariés / visiteurs ou de matériels acquis et déployés par l'entreprise, la présence de ces objets connectés se multiplie dans le monde professionnel.

Les objets connectés sont également de plus en plus utilisés pour des applications industrielles (afin d'optimiser la traçabilité des marchandises et la logistique, par exemple). On parle désormais d' « Industrie 4.0 » avec des usines connectées et « intelligentes » pour gagner en compétitivité.

Mais ces équipements présentent des vulnérabilités intrinsèques et des risques liés aux nouveaux usages rendus possibles grâce à une connectivité quasi continue à Internet.

Voici deux exemples représentatifs de ces nouveaux scénarii de menaces :

Exemple 1 : Augmentation de la surface d'attaque des entreprises

De plus en plus d'entreprises françaises s'équipent avec du matériel « connecté » dédié à la sécurité physique (alarme, détecteur de fumée, serrure, caméra de vidéo-protection, etc.). Ces systèmes sensibles sont reliés aux réseaux informatiques de l'entreprise voire accessibles depuis Internet.

Ces équipements de sécurité présentent également des failles de sécurité (identifiant et mot de passe par défaut, protocoles de communication non chiffrés, interface d'administration exposée à Internet, etc.) les exposent à des attaques informatiques. Ces dernières peuvent être exploitées dans le but de désactiver l'équipement mais également pour servir de point d'entrée pour réaliser une intrusion plus classique dans les réseaux informatiques de l'entreprise.

Le risque est d'autant plus grand qu'identifier des objets connectés vulnérables est facilité par des sites Internet comme *Shodan.io* ou *Censys.io*, des moteurs de recherche spécialisés qui référencent tout type d'équipement connecté à Internet.

Exemple 2 : Piratage d'une montre connectée

Des chercheurs en sécurité informatique ont montré qu'il était possible de compromettre à distance des montres connectées afin de prendre le contrôle de leurs capteurs (microphone, mesure du rythme cardiaque, etc.) ou d'accéder aux données échangées entre la montre et le smartphone auquel elle est reliée.

Commentaires

Le nombre d'objets connectés en circulation à travers le monde explose depuis quelques années. Estimé à 15 milliards aujourd'hui, ce chiffre pourrait atteindre les 80 milliards en 2020.

Ces objets connectés collectent et génèrent un nombre très important de données à caractère personnel qu'il est difficile de maîtriser et de sécuriser. Conçus généralement sans intégrer de façon native de mécanismes de sécurité (chiffrement par exemple), ils présentent également des vulnérabilités intrinsèques qui sont autant de portes d'entrée dans les réseaux informatiques des entreprises.

Si l'utilisation d'objets connectés dans un contexte professionnel peut permettre d'améliorer la compétitivité de l'entreprise, des mesures doivent être prises pour anticiper et prévenir les nouveaux risques qu'un usage non maîtrisé peut entraîner.

Préconisations de la DGSI

Afin de réduire les risques liés à l'utilisation d'objets connectés en milieu professionnel, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

- Recenser et réaliser une veille sur les vulnérabilités des objets connectés en activité dans l'entreprise ;

- Interroger les fournisseurs d'objets connectés sur les mesures de sécurité implémentées dans leurs produits :

  - Si c'est possible, il est recommandé de réaliser ou de faire réaliser un comparatif de différents modèles d'objets connectés en intégrant une évaluation technique de son niveau de sécurité.

- Encadrer l'usage des objets connectés personnels dans une charte de bonnes pratiques ou dans la politique de sécurité des systèmes d'information (PSSI) ;

- Réaliser une analyse de risque avant d'autoriser et de déployer des objets connectés sur les systèmes d'information de l'entreprise ;

- Créer des réseaux Wi-Fi ou filaires dédiés et cloisonnés à l'utilisation des objets connectés.
- Désactiver l'interface d'administration sur Internet, si elle est proposée par le fournisseur du produit :

  - Changer les mots de passe par défaut, le cas échéant.

- Déployer régulièrement les mises à jour des produits, quand celles-ci sont proposées par le fournisseur ;

- Sensibiliser les utilisateurs aux vulnérabilités qui sont liées aux objets connectés et notamment sur les données à caractère personnel qu'ils collectent, génèrent et transfèrent sur des services Cloud.