Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 49 – Janvier 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°49 Janvier 2019

Les vulnérabilités induites par l'utilisation d'objets connectés en milieu professionnel

Considérés comme la troisième révolution du numérique, les objets connectés (IoT ou internet des objets) sont des objets physiques équipés de capteurs (qui génèrent des données de différentes natures) auquel est associé une connexion à Internet, permettant la remontée de ces données dans le réseau. Ils sont généralement pilotables à distance à travers une interface (souvent une application mobile dans le cas d'objets grand public)[1].

Il s'agit parfois d'équipements personnels (bracelets, montres, cigarettes électroniques, etc.) apportés et utilisés au sein des locaux de l'entreprise par les salariés / visiteurs, mais aussi de matériels à usages industriels, notamment afin d'optimiser la traçabilité et la logistique des marchandises.

Ces équipements comportent néanmoins des vulnérabilités intrinsèques et génèrent des risques liés à leur connexion à Internet.

PREMIER EXEMPLE

Une entreprise extra-européenne propose à ses clients, parmi lesquels figurent des sociétés françaises, un accès à sa plateforme opérée à distance. Celle-ci permet de stocker d'analyser et de gérer en temps réel les données issues des capteurs industriels connectés. Les clients peuvent ainsi en théorie développer grâce à cet outil des solutions adaptées à leurs problèmes, et ce en toute autonomie.

Or, l'entreprise étrangère conserve l'intégralité du contrôle de cette plateforme, tout en bénéficiant des données collectées et des applications développés par ses clients.

Au-delà des risques de captation de données et de dépendances techniques et commerciales susceptibles d'en découler, ce type de solution connectée confère à son détenteur, ou à toute personne susceptible d'y accéder, l'opportunité d'identifier les processus industriels clés des clients et leurs vulnérabilités grâce à l'analyse des flux de données, et la possibilité d'influer sur le

[1] Étude « *Marchés des objets connectés à destination du grand public* » du PIPAME (DGE), 2018 : https //www.entreprises.gouv.fr/etudes-et-statistiques/marches-des-objets-connectés-a-destination-du-grand-public.

paramétrage des processus industriels des utilisateurs, à des fins de déstabilisation, voire de sabotage.

DEUXIEME EXEMPLE

De nombreuses 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, et peuvent être 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 reliée à Internet, etc.) qui les exposent à des attaques informatiques. Ces vulnérabilités peuvent être exploitées aux fins de désactiver l'équipement, mais également comme vecteurs d'accès aux réseaux informatiques de l'entreprise.

Ce risque est accru par la possibilité d'avoir recours à certains sites Internet ou moteurs de recherche spécialisés qui référencent tout type d'équipement connecté à Internet.

TROISIEME EXEMPLE

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.

Ces vulnérabilités pourraient être utilement exploitées à des fins malveillantes en direction d'un salarié préalablement ciblé d'une entreprise sensible, et donner accès à certaines de ses informations stratégiques.

COMMENTAIRES

D'après les travaux de l'IDATE DigiWorld[2], 35 milliards d'objets seront connectés à Internet d'ici à 2030 dans le monde.

L'utilisation exponentielle d'objets connectés entraînant mécaniquement une augmentation des volumes de données, les entreprises vont devoir améliorer leur capacité à les exploiter. La question

[2] Étude « *Marchés des objets connectés à destination du grand public* » du PIPAME (DGE), 2018 : https //www.entreprises.gouv.fr/etudes-et-statistiques/marches-des-objets-connectés-a-destination-du-grand-public.

du traitement et de la protection des données personnelles, générées massivement, apparaît dans ce contexte incontournable, alors même que le Règlement général sur la protection des données est entré en application le 25 mai 2018.

Par ailleurs, conçus généralement sans intégrer de façon native des mécanismes de sécurité (chiffrement par exemple), ils présentent des vulnérabilités permettant d'accéder aux réseaux informatiques des entreprises.

PRECONISATIONS 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 :

Pour les objets connectés industriels :

- **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 possible, réaliser ou de faire réaliser un comparatif de différents modèles d'objets connectés en intégrant une évaluation technique de leur niveau de sécurité.

- **Engager 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** à l'utilisation des objets connectés **et cloisonnés**.

Pour les objets connectés grand public :

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

- **Sensibiliser les salariés aux vulnérabilités** liées aux objets connectés et notamment sur les données à caractère personnel qu'ils sont amenés à collecter, générer et transférer sur des services de Cloud.

D'une manière générale :

- **Désactiver l'interface d'administration sur Internet**, si elle est proposée par le fournisseur du produit. **Changer** le cas échéant **les mots de passe par défaut**.

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

- **Consulter**, entre autres, la fiche pratique « ***Objets connectés : Les risques à connaître*** »[3] de la **Direction générale de la concurrence, de la consommation et de la répression des fraudes**, le site de la **CNIL**[4] , et celui de l'**ANSSI**.

[3] https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/objets-connectes.
[4] https://www/cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser.