Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 08 février 2016
N° CERTFR-2016-ACT-006

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-006

1 - Risques liés à l'utilisation d'objets connectés sur un réseau d'entreprise

Introduction

Depuis plusieurs années, la tentation d'utiliser des objets connectés sur un réseau d'entreprise s'amplifie. Bien évidemment, on pense en premier lieu aux téléphones intelligents, mais également à une multitude d'objets issus du phénomène de l'Internet des Objets ("Internet of Things" ou IoT en anglais). Le déploiement d'ampoules connectées permettrait ainsi de mieux maîtriser la consommation énergétique de l'entreprise, tout en instaurant une ambiance propice au travail. De même, qui n'a pas rêvé de disposer d'une cafetière ou d'une bouilloire connectée, déclenchable à distance au moment du départ du domicile et qui serait prête dès l'arrivée au bureau ? Cependant, la plupart de ces objets ont été conçus dans une atmosphère où la créativité primait sur la sécurité : il en résulte un niveau de sécurité très variable, comme l'illustre la série de vulnérabilités qui ont été récemment annoncées sur ce type d'équipements. Enfin, après avoir ciblé le secteur des particuliers, les constructeurs s'orientent de plus en plus vers le marché des entreprises, voire du commerce "business to business". L'étude des risques et contremesures associés à l'utilisation de ces objets connectés est donc primordiale pour ne pas affaiblir la sécurité globale du système d'information.

Caractérisation des risques

L'utilisation d'objets connectés implique de nouveaux risques, au niveau des données manipulées et des vulnérabilités introduites par ces systèmes.

Traitement des données à caractère personnel

Les objets connectés peuvent collecter un nombre important de données à caractère personnel. Ces données peuvent aller de l'état de santé d'une personne (dans le cas d'un bracelet connecté par exemple), jusqu'aux empreintes digitales des propriétaires (pour une serrure connectée par exemple). Ces données peuvent être stockées localement sur les systèmes, mais aussi être exploitées par des solutions en infonuage. Par exemple, certains systèmes de vidéosurveillance personnelle ou professionnelle stockent les enregistrements sur Internet sans protection. Dans la mesure où il s'agit de données à caractère personnel, il est donc important de s'assurer de leur confidentialité.

Introduction de vulnérabilités

Les systèmes embarqués dans les objets connectés sont généralement difficiles d'accès, et il est ainsi compliqué de les intégrer dans un processus de sécurisation. Les mises à jour de tels systèmes étant peu fréquentes, l'impact d'une vulnérabilité telle que *Heartbleed* ou *Shellshock* est très important. Cet impact est encore plus important quand ces objets connectés sont reliés à un réseau critique, tel qu'un système de contrôle industriel ou une voiture.

Exploitabilité

De plus en plus d'acteurs malveillants s'intéressent à l'exploitation des vulnérabilités présentes sur les objets connectés. Certains moteurs de recherche permettent d'identifier celles-ci sur Internet, et donc de prendre le contrôle des systèmes vulnérables. Dans ce contexte, un objet connecté peut servir de point d'entrée ou de rebond au sein d'un réseau.

Contremesures

Pour les constructeurs, afin de lutter contre les cybermenaces apportées par l'utilisation d'objets connectés, il est essentiel d'intégrer la prise en compte de la sécurité dès leur conception. Dans le cadre des objets connectés déjà en exploitation, il est important de mettre en place des mesures permettant de contrôler les données personnelles et techniques manipulées, afin d'éviter d'en perdre le contrôle. De même, l'application des mises à jour de sécurité, si possible, permet de corriger les vulnérabilités présentes dans ces systèmes. Enfin, il est conseillé de ne pas connecter ce type d'équipements sur les systèmes d'information critiques.

Conclusion

Le CERT-FR recommande la plus grande prudence vis-à-vis de l'apport des objets connectés dans un réseau d'entreprise.

Documentation

- http://www.globalsecuritymag.fr/Objets-connectes-et-securite,20160204,59465.html
- https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf
- http://tv.bpifrance.fr/Securite-des-objets-connectes_v2267.html

2 - Rappel des avis émis

Dans la période du 01 au 07 février 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-044 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-045 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-046 : Multiples vulnérabilités dans Asterisk
- CERTFR-2016-AVI-047 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-048 : Multiples vulnérabilités dans WordPress

Gestion détaillée du document

08 février 2016 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-006`