L'Internet des objets, une menace de plus pour les entreprises ?

L'Internet des objets (IoT) constitue-t-il une menace supplémentaire pour la sécurité des entreprises ? *« Oui*, répond sans hésiter Alain Merle (4e sur la photo en partant de la gauche), responsable des programmes sécurité au CEA-Leti. *Les dizaines de milliards d'objets qui seront connectés en 2020 vont augmenter les surfaces d'attaques. » « Le phénomène est très inquiétant avec l'IoT*, renchérit Bernard Barbier (1er sur la photo), aujourd'hui RSSI de Capgemini et ancien directeur technique de la DGSE, *car la surface d'attaque est en train de doubler ou tripler. »*

Pas armé face à la déferlante de l'IoT

Les deux hommes intervenaient lors de la table ronde « Sécurité des systèmes connectés : quelles bonnes pratiques à adopter ? » organisée dans le cadre de l'édition 2015 de Cap'Tronic, le programme d'accompagnement des PME pour l'intégration des solutions électroniques et logicielles dans leurs produits, qui se déroulait ce lundi 21 septembre à la Cité Internationale Universitaire de Paris. Une menace d'autant plus inquiétante que *« l'on n'est pas armé face à cette déferlante*, estime Alain Merle, que ce soit technologiquement ou en termes d'usages. *La cryptographie n'est pas la solution miracle, il y a des limites internes d'implémentation ajouté à un phénomène d'échelle plus complexe à gérer quand on doit faire face à des milliards d'objets au lieu de quelques dizaines de milliers. »*

Au delà des normes et des contraintes, la labellisation pourrait s'inscrire comme une partie de la réponse à la problématique de la sécurité des entreprises qui seront inévitablement confrontées à l'IoT pour assurer leur développement. *« On travaille beaucoup sur la certification des objets »*, indique Guillaume Poupard (2e sur l'image). Le directeur général de l'Anssi (Agence nationale de la sécurité des systèmes d'information) reconnaît néanmoins que le niveau de protection des objets est différent selon qu'ils concernent des systèmes stratégiques ou des usages grand public. Pour lui, *« il faut positionner la sécurité en fonction de l'état de l'art »*.

La sécurité dès la conception des objets

Pierre Girard (3e), expert en sécurité chez Gemalto invite de son côté les entreprises à prendre en compte la sécurité dès la conception de l'objet. *« C'est plus facile à gérer dès le départ qu'en rajoutant une couche de sécurité après coup et il faut assurer cette sécurité tout au long du cycle de vie de l'objet, sur 10 ou 15 ans, à travers les mises à jour et en assurant la surveillance face à l'évolution des attaques. »* Une conception initiale qui entraine un surcoût. *« La sécurité a un coût mais l'absence de sécurité coûte encore plus cher »*, justifie l'expert. Et d'illustrer son propos en citant l'exemple de Chrysler obligé de rappeler 1 million de véhicules suite à la démonstration de piratage d'une Jeep Cherokee qui va lui coûter quelque 1,4 milliard de dollars en frais de traitement.

Un risque loin de la problématique des PME par définition de tailles plus modestes que les constructeurs automobiles ? Bien au contraire. *« Les PME sont les cibles les plus touchées par les tentatives d'attaques. Il n'est pas question pour elles de devenir expertes en sécurité mais d'appliquer des règles de base, tels les mots de passe renforcés, la protection des réseaux Wifi, la séparation des usages professionnels et personnels, notamment avec les smartphones*, insiste Guillaume Poupard qui en a profité pour brandir à la salle quasi comble le guide des bonnes pratiques de l'informatique édité par l'Anssi. *Les chemins d'attaque passent souvent par les système personnels, que ce soit celui des employés ou des dirigeants. Le même mot de passe employé pour les usages professionnels et personnels est une réalité aujourd'hui. »*

Le RSSI, un gestionnaire des risques

D'où l'importance de revoir l'approche de la sécurité par de nouvelles (bonnes) pratiques. *« Avant le RSSI (responsable de la sécurité des systèmes d'information, NDLR) était un technicien. Aujourd'hui, c'est un métier de gouvernance, de dialogue et même de ressources humaines pour former les salariés »*, rappelle Bernard Barbier. Il est d'autant bien placé pour le savoir que le responsable a réalisé un petit test en interne en organisant une fausse campagne de phishing par e-mail invitant les collaborateurs à cliquer sur un lien potentiellement infectieux. *« Je ne vous donnerai pas le chiffre mais le taux de réussite [de l'opération] était élevé. »* Si même dans une SSII comme Capgemini cette technique d'attrape-nigaud fonctionne efficacement, que penser des autres secteurs ? Et d'admettre en conséquence que *« on s'est trompé à vouloir mettre toute la sécurité dans la technique. La technologie c'est 60% de la solution mais il reste 40% d'humain. La sécurité est une gestion des risques »*.

De son côté, Pierre Girard évoque un système de bons points attribués aux fournisseurs via un processus de labellisation et de certification pour simplifier la compréhension auprès des entreprises qui implémentent des solutions comme du grand public. Un point partagé par Alain Merle pour qui *« pour implanter la sécurité correctement, il faut penser certification »*. Un travail pour l'Anssi dont Guillaume Poupard annonce que des labellisations sont en cours, notamment pour les opérateurs de services Cloud d'infogérance en sécurité. Pour le directeur, *« il faut permettre à la sécurité d'apporter un plus, et non pas d'être un frein, pour faire en sorte que les technologies continuent de poursuivre leur développement de manière illimitée »*.

Lire également
La sécurité de l'Internet des objets insuffisante… selon un consortium IoT
Securitas Direct : Oracle scrute des millions de signaux d'objets connectés
Quiz Silicon.fr – L'Internet des Objets en 10 questions