AVIS D'EXPERT

Malakoff, le 1 février 2016

La face cachée des objets connectés : un point de vigilance à prendre en compte

L'internet des objets (IoT) n'est plus un simple effet de mode réservé à quelques Geek. Ce phénomène de société a profondément transformé nos usages et notre quotidien. Les objets connectés vont connaître une très forte croissance sur les prochaines années : d'après Gartner, le nombre d'objets connectés en circulation devrait passer de 4,9 milliards à 25 milliards en 2020. Si on ne peut que se réjouir des avantages que ces objets vont offrir à leurs utilisateurs, il faut prendre conscience que l'utilisation accrue de l'IoT implique de faire preuve d'une vigilance importante.

C'est notamment le cas des données recueillies par ces objets. Le traitement et l'utilisation de celles-ci font l'objet d'un grand « flou » qui se révèle être une source de préoccupation sérieuse. En effet, la valeur des données collectées est un point clé qui peut amener à de nombreuses dérives. La sécurité des données est donc stratégique et doit être prise au sérieux par les utilisateurs qui doivent être conscients de l'usage qui peut être fait de leurs données personnelles. A ce niveau, nous pouvons déceler deux grandes préoccupations :

L'utilisation des données à des fins commerciales

La première des motivations est de monétiser les données des consommateurs, de les utiliser ou de les revendre à des tiers (à des partenaires par exemple). Afin de donner plus de crédibilité à notre propos, imaginons l'intérêt des assureurs pour des données remontant d'applications et d'objets connectés liés à la santé. De telles informations pourraient, par exemple, fortement influer sur le montant des primes d'assurance. Cet exemple a le mérite d'être particulièrement parlant et démontre clairement que les données récoltées via les objets connectés peuvent avoir des répercussions. Le problème est aussi renforcé par le manque d'information donnée au consommateur qui va rapidement valider les contrats de licence et CGV sur son smartphone sans prendre le temps de se poser la question de l'usage de ses données personnelles…

L'utilisation malveillante des données

Il s'agit, à ce niveau, de réelles problématiques provenant du piratage massif des objets connectés. A la différence du cas précédent, nous nous trouvons ici dans un contexte particulièrement préoccupant qui peut avoir des conséquences sérieuses. Cela s'explique notamment par l'usage du smartphone qui occupe une place centrale dans le dispositif des objets connectés : avec notamment les applications bancaires ou gouvernementales qui permettent un accès sensible. En ce sens, le smartphone est une réelle porte d'entrée pour les pirates qui peuvent accéder à des informations précieuses et les détourner. Ce deuxième scénario est un risque majeur qu'il convient de prendre au sérieux pour ne pas se retrouver dans une situation embarrassante et préjudiciable.

Au regard de ces éléments, il est donc nécessaire de faire évoluer la législation pour d'une part protéger les utilisateurs d'objets connectés ainsi que leurs données personnelles et d'autre part s'assurer de son actualisation pour qu'elle suive au plus près les évolutions technologiques. En parallèle, il est crucial de sensibiliser les utilisateurs d'objets connectés sur la nécessité de mieux se renseigner sur l'usage de leurs données avant de souscrire à un service ou de télécharger une application. Ils devront également mesurer l'importance de la sécurisation maximale des dispositifs techniques et des devices qu'ils emploient quotidiennement.

Mathias LASNE
Directeur du Pôle Télécoms et Multimédia Groupe EOLEN

www.eolen.com

Contacts Presse

Franck Tupinier - Tél. : 06 74 68 37 93 - ftupinier@myntic-pr.com
Charlotte Lohou - Tél. : 01 46 12 10 34 - charlotte.lohou@eolen.com

Mathias LASNE
Directeur du Pôle Télécoms et Multimédia Groupe EOLEN