Les objets connectés ont de véritables problèmes en matière de sécurité

Les objets connectés ont de véritables problèmes en matière de sécurité

Connexions Bluetooth bavardes, chiffrement de piètre qualité, politiques de protection des données personnelles inexistantes… Les accessoires connectés ont tendance à vous mettre à nu.

Votre dernière course en forêt, vos déplacements à l'étranger, vos phases de sommeil, votre consommation en nicotine ou alcool, vos cycles de menstruations (si vous êtes une femme), votre pression artérielle, votre activité sexuelle… Pour toute activité personnelle, il y a désormais une application mobile et un accessoire connecté pour capter ces informations, comme par exemple le Nike Fuel Band. Et les utilisateurs en raffolent, si l'on croit les analystes. Selon Pew Research Center, plus de 60 % des Américains utilisent ces outils pour améliorer leur performances sportives ou préserver leur bonne santé. D'ici à 2018, le nombre de ces accessoires connectés devrait dépasser les 485 millions d'unités. Un marché en plein boom que tous les grands acteurs cherchent à accaparer, à commencer par Google et Apple.

Mais ce marché est encore très balbutiant, et notamment en matière de protection de données personnelles. Symantec vient de publier, il y a quelques jours, un rapport d'analyse qui évalue le niveau de sécurité de tous ces engins. Résultat: la plupart des applications révèlent des failles flagrantes permettant à des tiers de récupérer des données à l'insu des utilisateurs. Une majorité des bracelets peuvent être localisés grâces à leurs puces Bluetooth. Activés en permanence, ils sont plutôt bavards et émettent une adresse physique de type MAC, ainsi que des identifiants divers et variés, qu'il est aisé de capter dans un rayon de 100 mètres.
C'est d'ailleurs ce que les analystes de Symantec ont fait: ils ont créé des sniffeurs Bluetooth basés sur une carte Raspberry Pi, qu'ils ont disséminés aux abords d'une compétition sportive, ou trimballés dans un sac à dos en plein milieu d'un centre commercial. Certes, ces données ne permettent pas d'identifier une personne, mais c'est un premier pas…

Des mots de passe transmis en clair
Autre problème: parmi les applications qui utilisent des services cloud pour stocker ou traiter les données captées, 20 % transmettent les identifiants en clair, sans aucun chiffrement. Parmi les 80 % restantes, certaines appliquent aux identifiants des fonctions de hachage de faible protection comme MD5, qui peut facilement être craqué par les cybercriminels.
Dans un certain nombre de cas, la gestion de sessions laisse également à désirer, permettant par exemple de deviner ou de calculer des identifiants et ainsi d'accéder à des comptes utilisateurs.
Enfin, plus de la moitié des applications (52 %) n'apportent aucune information sur la manière dont toutes ces données sont traitées et stockées, alors que c'est obligatoire dans bon nombre de pays. Et quand il existe un document d'information, celui-ci est souvent très vague. On peut donc douter du sérieux de ces fournisseurs en matière de protection des données personnelles.
En somme: si toutes ces nouveaux appareils et applications semblent bien pratiques, il est conseillé de regarder en détail leur fonctionnement, histoire de pas se faire avoir !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/624818/les-objets-connectes-sont-des-passoires-en-matiere-de-securite/#?xtor=EPR-1-NL-01net-Actus-20140806