Bracelets connectés : l'étude qui révèle comment ils mettent en péril votre vie privée (même déconnectés)

Jean-Paul Pinte met en garde contre les failles et risques liés à l'utilisation du bracelet électronique, et esquisse des solutions pour se prémunir contre les atteintes à notre vie privée.

Avec Jean-Paul Pinte

Atlantico : Une étude du groupe de recherche *Open Effect* vient de montrer que les entreprises produisant des bracelets connectés étaient particulièrement laxistes en matière de sécurité de l'information privée. De quel type de faille parle-t-on?

Jean-Paul Pinte : 2015 aura vu le premier piratage d'une voiture de série permettant de désactiver ses freins ou encore d'éteindre son moteur à distance pendant qu'elle roule. Heureusement, ce piratage a été réalisé par des chercheurs en sécurité sans intention de nuire.

"Cette démonstration montre la vulnérabilité des véhicules qui sont aujourd'hui des objets connectés comme les autres mais où les conséquences d'une attaque peuvent être beaucoup plus graves" analyse Gérôme Billois, expert en cyber sécurité au cabinet Soluco dans une conférence thématique du CLUSIF le 14 janvier 2016.

L'année dernière a vu la multiplication des cas d'attaques réussies sur des objets connectés divers et variés tels que des poupées, des fusils de snipers, des *babyphones*, ou encore des pompes à insuline.

Dans ce décor ces trois dernières années les bracelets connectés ont principalement pris leur essor chez les sportifs et les pratiquants du running et de la course à pied.

Ces bracelets qui ont l'apparence pour certains d'un bijou sont capables de récupérer, de visualiser et d'analyser des données de vos diverses activités quotidiennes : pas effectués, distances parcourues, temps de sommeil et qualité de celui-ci, calories brûlées, suivi de l'alimentation…

Ainsi le "*Quantified Self* ou QS" est devenu une tendance. Ce mouvement permet à chaque personne de mesurer ses données personnelles, de les analyser mais aussi de les partager grâce à des objets connectés. On peut parler également de *Self Tracking* pour désigner ce genre de pratique.

Mieux connaître son corps grâce au suivi de certaines données liées à l'activité physique quotidienne est une bonne chose. On sait déjà que des applications ne manquent pas à ce jour dans ce domaine sur les smartphones pour partager ses performances et ses itinéraires (*Runstatic*), ce qui n'est pas sans risque pour celui qui ne connait pas l'envers du décor et donc les risques encourus

Les constructeurs comme pour l'Internet en son temps n'ont pas forcément pensé la sécurité car l'innovation est toujours trop belle sur le coup et doit laisser place au plaisir, à l'épatement et surtout à la course incessante à la technologie. Ils sont ainsi déjà en pleine réflexion, je le pense, sur l'analyse prédictive, préventive, personnalisée et participative de ces objets.

Certaines personnes plutôt mal intentionnées comme pour la cybercriminalité pourraient dans l'attente en profiter pour s'adonner à la captation de données totalement possible depuis longtemps et profiter ainsi du partage de données que proposent ces objets connectés.

L'internet des objets ou le Web 4.0 sera rempli de capteurs et il a déjà prouvé qu'il était difficile d'éviter des fuites de données personnelles via Bluetooth ou Wifi même si votre ordinateur ou smartphone étaient fermés.

Il en va de même des objets connectés qui pourraient ainsi payer les frais de leur interconnexion à venir. Tout ceci nous échappe et nous dépasse même. Il en va même de notre réputation sur la toile. Peu de gens mesurent leur ADN numérique et sont capables aujourd'hui de dresser une cartographie des fruits de leurs pérégrinations sur la toile et encore moins des informations déposées ou relayées à leur insu sur d'autres espaces indélébiles. Aujourd'hui parmi les constructeurs (Fitbit, Garmin, Jawbone, Mio, Withings et Xiaomi) seul Apple semble adopter un discours plus clair sur les concepts de vie privée et de sécurité. Il a notamment adopté la norme de la vie privée *Bluetooth*.

L'objet connecté est-il un cheval de Troie supplémentaire pour *Big Brother* ? Quelle utilité pourrait-on tirer d'un bracelet ouvert à une certaine malveillance numérique ? De quels dangers parle-t-on ?

"L'Internet des objets va générer des données, beaucoup de données, notamment personnelles, ce qui explique que les grands groupes américains investissent beaucoup dans ce domaine, explique Samuel Ropert, consultant pour IDATE. Le but est de collecter de plus en plus de données, afin d'offrir de nouveaux services et de les monnayer."

C'est ainsi que les dispositifs présents sur les bracelets connectés collectent aujourd'hui vos performances et votre état de santé cardiaque par exemple, ils collectent également des informations personnelles, comme le nom, l'âge et le sexe, ce qui peut être divulgué par Wi-Fi.

Il y a comme pour toute application que vous installez sur un smartphone une transmission de données entre l'appareil et une application connexe ou Internet. Données obligatoirement transmises à un tiers. On sait que presque 40 % de ces applications ont ensuite accès à vos appartenances et interactions sur les réseaux sociaux par exemple. A titre d'exemple des *trackers* permettent de surveiller l'emplacement de votre appareil connecté même surtout s'il s'agit d'un appareil installé chez vous, Bluetooth ou non activé. Ces données générées peuvent même faire l'objet de falsification, d'une désinformation, voire encore de vol de données vous concernant.

Cette traçabilité des données captées peut aussi être utile à certains cyber(délinquants) en quête de rencontres lorsqu'ils connaissent, par exemple, l'itinéraire habituellement suivi par une personne. D'autres pourraient "s'amuser" sous peu à intervenir sur la tension artérielle et le pouls des adeptes de ces bracelets pour augmenter la tension artérielle et le pouls par exemple… Des attaques ont en effet déjà eu lieu sur des pacemakers et des systèmes de dialyse alors pourquoi pas sur des bracelets connectés)

Les compagnies d'assurance pourraient aussi bientôt en France s'intéresser à vos données et en savoir bien plus sur votre santé pour reparler de vos contrats, ce qui n'est pas sans évoquer l'éthique autour de ces technologies nomades.

De nombreux bracelets connectés font heureusement preuve d'une prise en compte d'une certaine sécurité comme le démontre cette étude d'AV-TEST.

Quelle sont les possibilités pour se protéger de telles malveillances aujourd'hui? Doit-on se méfier de tels objets?

Se protéger dans cette société hyper connectée relève de l'impossible ou alors d'une attention sans relâche de la part des détenteurs d'objets connectés comme les bracelets. Il faudrait déjà que les utilisateurs prennent le soin de se documenter sur l'objet en question, voire en lire ne serait-ce que sa notice d'utilisation.

On ne pourra éviter le développement de telles technologies. Les traqueurs d'activité représentent la deuxième catégorie de produits la plus importante en termes de part de marché (33% contre 46% pour les montres) et en sont conscients. Cette position s'explique du fait de la notoriété de son principal concepteur, Nike. Celui-ci a grandement participé à la démocratisation des traqueurs d'activités en les implantant directement dans les chaussures dédiées à la course à pied. Ces produits représentent un chiffre d'affaires de 20 millions d'euros pour l'année 2013 en France.

Comme il existe aujourd'hui un droit à l'oubli qui se met tout doucement en place dans le Web social (Web 2.0), on pourrait évoquer ici un droit au silence des puces qui serait une solution. Mais ne soyons pas dupes, enlever les capteurs ou toute puce à haute fréquence de tels systèmes reviendrait à se passer des atouts de ces objets connectés.

Le cadre juridique actuel n'est pas totalement adapté à la diversité des objets connectés.

Face à un tel développement et de telles interrogations, les 29 autorités européennes de protection des données ont publié un avis en octobre dernier. Avec un rappel des obligations faites aux constructeurs, les droits reconnus aux utilisateurs, et les mesures de sécurité à mettre en œuvre par les responsables de traitement.

Dans l'attente j'invite les utilisateurs de ces bracelets connectés à bien découvrir avant utilisation les interactions qu'ont leurs objets connectés au cyberspace tels les appels à participation à concours via des mails faisant le lien avec leurs bracelets, les partages de données via les réseaux sociaux les plus connus. Enfin, de modifier de manière régulière leurs mots de passe. On ne le répètera jamais assez !