Vous utilisez des objets connectés? Gare à vos données

Vous utilisez des objets connectés? Gare à vos données

Une étude publiée par l'entreprise de cybersécurité AV-Test montre que la plupart des objets connectés testés, destinés à surveiller sa forme, sont susceptibles d'être piratés.

Ils mesurent toutes les performances. Seulement voilà: d'après une étude publiée par l'entreprise de cybersécurité AV-Test le 18 juillet 2016, les objets connectés utilisés pour surveiller sa forme ne sont pas sécurisés. Pire encore, ils présentent des failles de sécurité pouvant permettre à des pirates informatiques d'accéder à leurs données et de les manipuler.

Des appareils utilisés par les assureurs

Pour en arriver à cette conclusion, AV-Test a examiné sept appareils utilisant Android, le système d'exploitation mobile de Google, et repéré des vulnérabilités similaires à celles qu'elle avait déjà identifiées il y a un an. Beaucoup d'appareils manquent de connexions sécurisées ou de protection contre les accès non autorisés. Les fabricants « ne font souvent pas assez attention à l'aspect de la sécurité », indique l'étude.

Elle fait pourtant valoir qu'il faudrait prendre davantage au sérieux la sécurité de ces appareils dont l'usage s'élargit, certaines assureurs santé commençant même à les utiliser pour fixer leurs tarifs ou proposer des remises.

Trois appareils avec des risques de piratages importants

Dans le détail, les appareils affichent des niveaux de sécurité variés. Selon l'étude, le risque le plus élevé est présenté par les appareils de Runtastic, Striiv et Xiaomi, où AV-Test relève 7 à 8 vulnérabilités potentielles sur un total de dix. AV-Test indique notamment que « ces appareils peuvent être suivis à la trace plutôt facilement » et qu'ils utilisent des systèmes d'identification et de protection contre les accès non autorisés incohérents ou inexistants, ou encore que leur programme n'est pas assez protégé pour garantir la sécurité des données collectées.

« Pire que tout, Xiaomi stocke toutes les données de manière non cryptée sur le smartphone », s'inquiète l'étude. Les appareils les plus sûrs, avec 2 à 3 risques potentiels pour la sécurité, sont la montre Pebble Time, le bracelet Band 2 de Microsoft et le moniteur d'activité et de sommeil Basis Peak.

L'Apple Watch tire son épingle du jeu

La montre connectée Apple Watch, évaluée selon des critères différents car elle utilise un autre système d'exploitation, a pour sa part, selon les chercheurs d'AV-Test, une « note de sécurité élevée », malgré des « vulnérabilités théoriques ».

L'Apple Watch est « presque impossible à suivre à la trace », mais dévoile certaines caractéristiques d'identification quand elle est en mode avion alors que ça « ne devrait pas être le cas », détaillent-ils. L'appareil « utilise essentiellement des connexions cryptées qui ont des sécurités supplémentaires », mais ses mises à jour se font par une connexion non cryptée, notent-ils aussi.

D'après le cabinet de recherche IDC, plus de 75 millions d'appareils connectés « fitness » ont été vendus en 2015 dans le monde, et le niveau devrait franchir la barre des 100 millions cette année.

Article original de Stephen Lam

Réagissez à cet article

Original de l’article mis en page : Vous utilisez des objets connectés? Gare à vos données – L’Express L’Expansion