Les experts de la sécurité se penchent sur la Watch d'Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de *The Register* ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « *le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil* ». Pour lui, il ne fait aucun doute que *« les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth* ».

Problème de confidentialité des données

Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « *Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés* ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

La fraude au paiement

En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?

Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « *Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser.* »

Cela passe pour lui par plusieurs axes : « *Chiffrement des données transitant sur le Bluetooth et la*

conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

A lire aussi :

Comment la CIA a mené campagne pour casser la sécurité d'Apple
Freak affaiblit le chiffrement des navigateurs Apple et Android