D’où vient le danger des Objets connectés ?

	D’où vient le danger des Objets connectés ?

Le développement des objets connectés s'accélère de plus en plus tandis que la mise en place de moyens de sécurité reste quant à elle beaucoup plus discrète… Tout le monde connaît le récit mythique du cheval de Troie, alors ne sommes-nous pas en train de danser sur ce qui va causer la perte de notre identité à chacun ? Qu'en est-il des normes de sécurité dans le domaine des objets connectés ? Comment pouvons-nous protéger nos données personnelles ?

Deux étudiants en médecine, ont pointé du doigt les failles que pourraient comporter certains objets connectés, dans des actions spectaculaires : prendre le contrôle d'un Pacemaker à distance ou encore désactiver les freins d'une voiture connectée. Ces actions coups de poing mettent à nu les faiblesses que comportent certains objets connectés face à des hackers malveillants. En effet, c'est précisément là que ce situe le paradoxe des nouvelles technologies qu'utilisent les objets connectés… Car s'ils sont conçus pour nous faciliter le quotidien, ils peuvent au contraire nous faire beaucoup de mal et en particulier à nos données personnelles ! Pour pouvoir se protéger, il faut avant tout comprendre cette technologie et adopter quelques habitudes très utiles.

Tout objet connecté peut être hacké

Pour comprendre comment une balance connectée peut devenir notre ennemi numéro 1, il faut d'abord comprendre comment cheminent des data (c'est-à-dire les données personnelles qui sont recueillies pendant l'utilisation de l'objet connecté) vous concernant, quels en sont les tenants et les aboutissants et où sont stocké ces données.
Il existe trois principaux canaux par lesquels voyagent nos data : les réseaux Wifi, le Bluetooth et les réseaux cellulaires pour objets connectés (Sigfox et Lora sont deux des principaux acteurs de ces réseaux).
Ces données sont ensuite acheminées jusqu'aux serveurs du fabricant ou du développeur de l'application pour ensuite revenir vers vous avant de repartir sur le Cloud… Au milieu de tous ces voyages, il devient très facile de voler ou de prendre le contrôle de vos objets, surtout si vous passez par un réseau public.

Le hackage est une menace très sérieuse à prendre en compte

En 2015, on a constaté une augmentation de 50 % de la cyber-criminalité en France ! Les concepteurs et développeurs d'objets connectés nous parlent sans cesse de nouveautés incroyables et parfaites pourtant comment celles-ci sont-elles sécurisés ? Est-ce que les différents fournisseurs appliquent ou suivent des normes ou une réglementation officielle pour sécuriser le matériel de fabrication ? Il semble qu'il n'y ai pas encore de législation officielle qui soit mise en place, même si la CNIL (Commission Nationale de l'Informatique et des libertés) s'est dernièrement attelé au sujet lors du Forum International de la cyber-sécurité.

Sécurité des objets connectés

C'est lors des voyages des data que celles-ci sont les plus vulnérables.
Mais le problème reste entier tant que les données qui voyagent ne seront pas cryptées… Ces données personnelles récoltés par les objets connectées peuvent avoir un intérêt économique pour certaines sociétés.
Ainsi, votre balance connectée peut en dire long sur vos habitudes alimentaires, votre traqueur de sommeil connecté peut donner, lui aussi, de précieuses informations sur vos habitudes de vie quotidienne. Ces données qui peuvent se monnayer très cher favorisent le profilage ciblé pour les publicités notamment et vous enlever petit à petit la liberté d'acheter ce qui vous plaît et non pas ce que l'on vous a suggéré. Le reste des data qui vous concerne, comme vos données bancaires ne sont, également, pas à l'abri d'un hackeur qui chercherait à vous voler de l'argent sans toucher à votre porte-monnaie !

Optimisez la sécurité de vos objets connectés

Face aux deux risques majeurs de la reprise malveillante de vos données personnelles : l'utilisation commerciale et le piratage des donnés personnelles, vous pouvez adopter quelques gestes simples pour augmenter la sécurité de vos data. Si les objets connectés s'avèrent être dans de nombreux cas, un formidable assistant dans la vie quotidienne pour surveiller votre alimentation, votre sommeil, … Au contraire, s'ils sont mal connus ou utilisés d'une mauvaise manière, ils peuvent devenir très dangereux pour le particulier. Vous ne devez pas oublier qu'il est essentiel de comprendre comment fonctionnent ces technologies pour en profiter au maximum sans crainte.
Dans un premier temps, vous devez lister tous les objets connectés en activité dans votre maison et déterminer pour chacun d'entre-eux à quoi ils sont connectés et par quel biais (Wifi ou Bluetooth ou réseau cellulaire). Par cet inventaire un peu minutieux mais très utile, vous pourrez contrôler le cheminement de vos données personnelles et savoir quel objet connecté communique par des biais peu sécurisés. Pour que votre sécurité soit optimale, vous devez également effectuer régulièrement des mises à jour en ce qui concerne la sécurité et surtout changer régulièrement les mots de passe et vos identifiants. Il ne faut pas oublier que même si vos objets connectés restent dans votre maison, les data qu'ils produisent voyagent eux sur le net et donc dans le monde !

Réagissez à cet article

Source : *IOT et sécurité : ne laissez plus le cheval de Troie entrer chez vous*