

La sécurité de l'Internet des objets insuffisante... selon un consortium IoT

La sécurité de l'Internet des objets n'est pas assurée, d'après l'organisation professionnelle **Online Trust Alliance** (OTA), qui vient de publier un [guide des bonnes pratiques](#) à l'attention des fabricants, des développeurs et des vendeurs d'objets connectés.

ADT, AVG Technologies, Microsoft, Symantec, TRUSTe et **Verisign** font partie du groupe de travail sur l'Internet des objets formé en janvier dernier au sein de l'OTA. Leur postulat est le suivant : la fiabilité de tout objet, application ou service connecté, dépend à la fois de la sécurité, de la protection des données privées et de la durabilité. Ce dernier critère concerne la gestion du cycle de vie d'un appareil connecté et la protection des données, y compris après la fin de la garantie.

Risque et durabilité des objets connectés

Trop souvent négligée, la durabilité des objets connectés est pourtant « *critique pour la sécurité, la confidentialité et la protection des utilisateurs et des entreprises dans le monde* », selon les auteurs du rapport. Si la durabilité est oubliée, ajoutent-ils, des dispositifs sécurisés à l'achat deviendront exposés au piratage au fil du temps. Des hackers pourraient alors ouvrir à distance les portes d'un garage, prendre le contrôle des moniteurs pour bébés ou encore saboter de multiples appareils connectés...

Pour éviter le pire, le groupe de travail de l'OTA recommande aux professionnels du secteur de :

- communiquer leur politique de confidentialité avant commercialisation du produit connecté ;
- crypter toutes les données personnelles échangées et stockées ;
- préciser les politiques de collecte de données avant l'achat ;
- indiquer si l'utilisateur peut supprimer ou anonymiser ses données avant de se débarrasser de l'objet connecté ;
- et, enfin, publier un calendrier dédié au support.

La Online Trust Alliance appelle les parties prenantes à [commenter ses propositions](#) d'ici au 14 septembre prochain.

Lire aussi :

[Black Hat : Transformer les objets connectés en radio espion](#)
[1 développeur sur 5 travaille pour l'Internet des objets](#)

crédit photo © Maksim Kabakou / Shutterstock