Plate-forme de politique de sécurité des objets connectés (IoT)

14 novembre 2019

Selon la plate-forme de politique de sécurité de l'IoT, les objets connectés (IoT, Internet of Things en anglais) recèle un potentiel considérable pour améliorer notre monde. Les projections concernant l'impact des objets connectés sur Internet et sur l'économie mondiale sont impressionnantes, et prévoient une croissance explosive du nombre d'appareils connectés, ainsi que leur utilisation dans un large éventail d'applications nouvelles et intéressantes. La déclaration qui suit s'adresse à tous les gouvernements, citoyens et organisations intéressés par la réalisation de ce potentiel des objets connectés.

Avec des milliards d'appareils, d'applications et de services connectés déjà utilisés et un nombre croissant de connexions en ligne, la sécurité des objets connectés est d'une importance capitale. Un grand nombre de ces appareils ne disposent pas de fonctionnalités de sécurité de base, et les vulnérabilités ou les appareils compromis peuvent être forcés de servir de points d'entrée pour les cyberattaques, mettant en danger les données sensibles et menaçant la sécurité des utilisateurs individuels. Ce sont là des risques auxquels les utilisateurs et les entreprises qui adoptent les objets connectés doivent faire face.

D'importants travaux sont déjà en cours pour traiter les risques et identifier les opportunités offertes par les objets connectés, car l'amélioration de la sécurité permettra aux consommateurs de tirer parti de leurs avantages. Compte tenu de la portée mondiale et de l'impact d'Internet, il est important d'unir nos efforts pour améliorer la sécurité des objets connectés.

À ce jour, nos agences et organisations gouvernementales ont créé ou sont à développer de solides cadres de sécurité pour les objets connectés, par le biais de recherches intensives, d'une collaboration et de forums multipartites. Les membres de la plate-forme de politique de sécurité des objets connectés soulévant la barre des pratiques de sécurité dans leurs domaines respectifs. Notre objectif est d'améliorer la sécurité de l'écosystème global des objets connectés.

Bien que ces cadres ne soient pas exactement identiques, chacun tente d'améliorer significativement la sécurité selon son propre contexte régional et national. Ces cadres ciblent différentes applications (consommateurs, industrie, etc.) et parties (réseaux, dispositifs, etc.) de l'écosystème des objets connectés, et explorent différentes approches pour mettre en place des recommandations et des pratiques exemplaires. Et pourtant, ces cadres ont certains principes en commun, notamment :

- S'assurer que la sécurité soit intégrée dans toutes les étapes de la conception, du développement, et du cycle de vie, y compris des évaluations des risques, des tests et des contrôles de sécurité ;

- Veiller à ce que les données personnelles et critiques soient protégées ;
- Faciliter la suppression des données personnelles par les utilisateurs.

Ces principes peuvent être atteints par différents moyens, notamment :

- Mettre en œuvre une politique de divulgation des vulnérabilités ;
- Expliquer clairement aux consommateurs la durée minimale pendant laquelle un appareil recevra les mises à jour de sécurité logicielles ;
- Fournir des mécanismes de mise à jour des logiciels sécurisée ;
- Avec des appareils auxquels les fabricants intègrent des mots de passe ou des identifiants uniques ;
- Protéger la communication des données de sécurité sensibles [par exemple au moyen de flux de données cryptées] ;
- Stocker de manière sécurisée les informations d'identification et les données sensibles en matière de sécurité.

Mais ces cadres ne sont qu'une première étape. Les membres de la plate-forme de politique de sécurité des objets connectés travaillent ensemble pour relever les défis mondiaux, en particulier la fragmentation, dans le cadre des efforts visant à créer une standardisation internationale de la sécurité des objets connectés.

À l'avenir, la plate-forme et ses membres devraient continuer de travailler à l'harmonisation et à l'élaboration de cadres lorsque cela s'avère nécessaire pour s'assurer qu'ils suivent le rythme d'un monde technologique en constante évolution, afin d'accroître la confiance et de sensibiliser aux mesures de sécurité associées aux objets connectés.