Plateforme de politique de sécurité des objets connectés (IoT)

14 novembre 2019

La "Plateforme de politique de sécurité des objets connectés" estime que les objets connectés (*IoT, Internet of Things*) recèlent un potentiel considérable pour améliorer notre monde. Les prévisions concernant leur impact sur Internet et sur l'économie mondiale sont impressionnantes. Le nombre d'objets connectés va croître de manière exponentielle ainsi que leur utilisation via un large éventail d'applications inédites et prometteuses. La déclaration qui suit s'adresse à tous les gouvernements, citoyens et organisations intéressés par ce fort potentiel et sa mise en œuvre concrète.

Avec des milliards d'appareils, d'applications et de services connectés déjà en service 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. Des failles ou des appareils infectés peuvent alors servir de points d'entrée pour des cyberattaques, exposant ainsi des données sensibles et menaçant la sécurité des utilisateurs. Ce sont là des risques auxquels les utilisateurs et les entreprises doivent faire face.

D'importants travaux sont déjà en cours pour remédier à de tels risques. L'amélioration de la sécurité permettra aux consommateurs de tirer parti de toutes les opportunités offertes par les objets connectés. Il est donc primordial d'unir nos efforts pour améliorer leur sécurité.

À ce jour, nos agences et organisations gouvernementales ont créé ou sont en train de développer de solides cadres pour la sécurité des objets connectés grâce à des recherches intensives, des collaborations et des forums avec l'ensemble des acteurs concernés. Les membres de la "Plateforme de politique de sécurité des objets connectés", dans leurs domaines de compétences respectifs, fixent la barre plus haut concernant ces pratiques de sécurité. Notre objectif : améliorer la sécurité de l'écosystème mondial des objets connectés.

Cependant, les cadres qui règlementent la sécurité des objets connectés ne sont pas exactement identiques. Chacun d'eux tente d'améliorer significativement le niveau de sécurité selon son propre contexte régional et national. Ils visent différentes applications (consommateurs, industrie, etc.) et parties de l'écosystème des objets connectés (réseaux, dispositifs, etc.). Ils explorent différentes approches pour mettre en place des recommandations et les meilleures pratiques qui soient. Ces cadres ont tout de même certains principes communs, notamment :

- s'assurer que la sécurité est prise en compte dans toutes les étapes de la conception, du développement, et du cycle de vie de l'objet connecté, avec notamment 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 réalisés par différents moyens, notamment :

- en instaurant une politique de déclaration des failles de sécurité ;
- en indiquant clairement aux consommateurs la durée minimale pendant laquelle un appareil recevra les mises à jour de sécurité logicielle ;
- en fournissant des mécanismes de mise à jour des logiciels sécurisée ;
- avec des appareils auxquels les fabricants intègrent des mots de passe ou des identifiants uniques ;
- en protégeant la communication des données sensibles [par exemple au moyen de flux de données cryptées] ;
- en stockant 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 "Plateforme de politique de sécurité des objets connectés" travaillent ensemble pour relever les défis mondiaux auxquels ils sont confrontés, 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 Plateforme et ses membres devront continuer de travailler à l'harmonisation et à l'élaboration de tels cadres lorsque cela s'avère nécessaire. En effet, ces derniers devront suivre le rythme d’un monde technologique en constante évolution afin d’accroître la confiance des utilisateurs et de les sensibiliser aux mesures de sécurité propres aux objets connectés.