Internet Society

Internet Society France Chapter

isoc.fr/iot

février 2020

GROUPE DE TRAVAIL POUR UN INTERNET DES OBJETS DE CONFIANCE

LES 22 RECOMMANDATIONS

D'ici à 2020, le nombre d'objets connectés pourrait osciller entre 30 milliards (Gartner) et 80 milliards (iDate).

L'Internet des objets pourrait être à l'origine de nombreuses opportunités et innovations dans des domaines aussi divers que la santé, l'environnement, l'agriculture ou les transports à condition de respecter les principes d'un numérique responsable, au service des utilisateurs et de l'intérêt général. **Nombre de ces objets sont conçus sans tenir compte, dès la conception, des règles de protection de la sécurité et de la vie privée des utilisateurs et arrivent sur le marché insuffisamment sécurisés.** Cela constitue une menace aussi bien pour l'utilisateur, que pour le réseaux, à travers le détournement d'objets connectés.

Convaincus qu'il faut renforcer la confiance des utilisateurs et faire en sorte que l'Internet des objets reste une opportunité, l'Internet Society et l'Internet Society France, ont constitué un groupe de travail composé d'experts issus de la société civile, des secteurs pubic comme privé, de la communauté technique et du monde académique.

Le groupe de travail pour un Internet des objets de confiance s'est donné pour mission depuis son lancement en janvier 2019 de renforcer la sécurité et la protection des données personnelles. Le groupe a choisi de s'intéresser à la situation en France, en s'inspirant des bonnes pratiques observées autant en Europe que dans le reste du monde et en prenant appui sur les initiatives similaires mise en place par l'Internet Society au Sénégal et au Canada.

Le groupe de travail pour un Internet des Objets de Confiance fait 22 recommandations.

Sécurité

- INTÉGRER UNE NOTICE DE SÉCURITÉ UTILISATEUR (changer fréquemment le mot de passe, limiter l'accès de l'objet connecté aux autres appareils électroniques, procéder aux mises à jour de sécurité...)
- CRÉER UN LABEL DE SÉCURITÉ DÉLIVRÉ OU AUTO-ÉVALUÉ pour toute mise sur le marché d'un objet connecté
- UTILISER EXCLUSIVEMENT DES MOTS DE PASSE ROBUSTES à l'exclusion des mots de passe par défaut
- GARANTIR LA SÉCURITÉ DES COMMUNICATIONS par le renforcement du chiffrement
- ASSURER L'INTÉGRITÉ PHYSIQUE DE L'UTILISATEUR

Transparence

- RENFORCER LA MAÎTRISE DES UTILISATEURS DES OBJETS CONNECTÉS en créant un droit à l'explicabilité et à la protection de l'attention
- INCITER LES FABRICANTS À S'INTERROGER sur l'adéquation des fonctionnalités installées et la finalité de l'objet connecté
- INFORMER CLAIREMENT L'UTILISATEUR afin de lui permettre un choix libre et éclairé
- PERMETTRE À L'UTILISATEUR DE DÉSACTIVER à tout moment l'appareil
- METTRE À DISPOSITION, AU PROFIT DE CHAQUE UTILISATEUR, UNE INFORMATION CLAIRE et facilement accessible par la standardisation d'une série de pictogrammes

Protection de la vie privée et des données personnelles

- METTRE EN PLACE UNE ÉVALUATION D'IMPACT SYSTÉMATIQUE SUR LA VIE PRIVÉE au stade de la conception de tout objet connecté
- LANCER UNE MISSION D'EXPERTISE SUR LA PROTECTION DES DONNEES DES UTILISATEURS à l'aune de l'internet des objets
- ÉTABLIR UN RÉGIME SPÉCIFIQUE DE RESPONSABILITÉ CIVILE pour les objets connectés
- ASSURER EN TOUTE TRANSPARENCE L'INFORMATION ET LA PROTECTION DES DONNÉES à caractère personnel des utilisateurs
- PORTER UNE ATTENTION TOUTE PARTICULIÈRE À LA PROTECTION DES DROITS DES MINEURS. Pour toute vente d'objet connecté destiné aux parents comme aux enfants, intégrer une notice de sécurité adaptée (explications en des termes simples, dessins...)
- AVOIR UNE APPROCHE INTERNATIONALE DE LA PROTECTION de la vie privée et des données à caractère personnel
- METTRE EN ŒUVRE UNE POLITIQUE DE DIVULGATION DES VULNÉRABILITÉS qui garantisse la protection du lanceur d'alerte.

Résilience, interopérabilité et durabilité

- MINIMISER L'IMPACT ENVIRONNEMENTAL des objets connectés
- PROPOSER DES MISES À JOUR qui tiennent compte de la durée de vie des objets connectés.
- INTÉGRER LA GESTION ET LA SUPERVISION DES VULNÉRABILITÉS dès la conception.
- GARANTIR UNE SÉCURITÉ DE BOUT EN BOUT ET UNE FIABILITÉ de l'objet connecté avec l'assurance d'une interopérabilité effective.
- PRÉVOIR ET INFORMER L'UTILISATEUR QUANT AUX POSSIBILITÉS DE RECYCLAGE de l'objet dans le respect d'un principe de gratuité ou de reprise par le fabricant.

Edité par l'Internet Society France, imprimé par nos soins. Rédaction : Lucien Castex, Nicolas Chagny. Mise en page : Cécile Bancal

Les présentes recommandations sont celles de l'Internet Society France et de l'Internet Society, sur la base des travaux du groupe dont les membres figurent sur isoc.fr/groupe-iot

isoc.fr/iot