CONFIANCE IOT PAR DISIGN

Le cadre de confiance de l'OTA IoT

L'avènement des objets connectés dans notre vie quotidienne apporte une promesse de commodité, d'efficacité et de perception, mais crée également une plate-forme de risque partagé. Gartner prévoit que plus de 20 milliards d'appareils seront connectés d'ici 2020. Depuis les trackers de fitness aux thermostats intelligents, en passant par les serrures et appareils, ces objets connectés (IoT) représentent un marché énorme et redéfiniront fondamentalement la manière dont les personnes interagissent avec le monde qui les entoure.

La confiance des consommateurs est essentielle pour que l'IoT prospère et grandisse. Cependant beaucoup de produits et services d'aujourd'hui sont lancés sur le marché au coût le plus bas possible avec une faible considération pour la sécurité de base et la protection de la confidentialité. Cela introduit différents niveaux de risque à la fois pour les utilisateurs et l'Internet lui-même - de la surveillance involontaire et la compromission des données au risque physique (les verrous intelligent, par exemple) aux caméras de sécurité utilisées dans le cadre d'un botnet pour attaque Internet. Par défaut, beaucoup recueillent de grandes quantités d'informations personnelles et sensibles qui peuvent être partagées et échangées sur le marché libre. La majorité de ces appareils n'a pas la fonctionnalité (ou une méthode facilement détectable) pour supprimer facilement ces données personnelles.

En l'absence d'adoption de normes de sécurité et de pratiques responsables en matière de protection de la confidentialité, nous arrivons à un carrefour où une réglementation peut être requise. Pourtant, en réalité, la législation en elle-même ne sera pas efficace. L'adoption de la réglementation prendra trop de temps et ne suivra jamais l'univers de menaces en constante évolution.

En réponse, plus d'une centaine de parties prenantes représentant l'industrie, le gouvernement et les défenseurs des consommateurs ont contribué à un ensemble d'actions de base recommandées dans le cadre de l'Online Trust Alliance (OTA) qui est maintenant une initiative de l'Internet Society. L'adoption de ce Cadre de confiance pour IoT augmente le niveau de sécurité des appareils IoT et des services associés pour mieux protéger les consommateurs et la confidentialité de leurs données. Le cadre sert à plusieurs fins puisqu'il :

- Guide la conception du fabricant et du fournisseur de services, ainsi que les choix de politique commerciale, depuis la conception initiale jusqu'au cycle de vie complet du produit,
- Fournit aux acheteurs et aux canaux de distribution les filtres appropriés pour évaluer la confidentialité et la sécurité, et
- Donne aux décideurs politiques les principes de sécurité nécessaires pour une revendication et une politique économique informée.

Bien qu'il existe d'autres cadres liés aux cadres IoT, ce cadre de confiance IoT est unique de deux manières significatives :

- **Il couvre la question de sécurité, de confidentialité et de durabilité à long terme (cycle de vie).** Beaucoup d'autres se concentrent uniquement sur la sécurité, l'interopérabilité ou la confidentialité, et peu prennent en compte les problèmes de cycle de vie associés à une maison intelligente ou que faire lorsque les mises à niveau logicielles ne sont plus disponibles pour un appareil à long durée de vie tel qu'un ouvre-porte de garage.

- **Il aborde de manière holistique l'ensemble de l'écosystème**. Cela inclut les appareils / capteurs, les applications mobiles et les services backend. La plupart des cadres se concentrent uniquement sur les appareils, mais un système n'est pas plus solide que son maillon le plus faible.

Le cadre comprend une liste de principes applicables dans huit catégories. Si ces principes sont respectés, ils peuvent réduire les risques pour la sécurité et la confidentialité, renforcer la confiance et permettre à l'écosystème IoT de se développer :

- **Authentification -** authentifier les appareils et les utilisateurs pour empêcher les accès malveillants.
- **Cryptage -** crypter de manière exhaustive les données afin d'empêcher l'écoute clandestine ou l'accès aux données sensibles.
- **Sécurité -** la sécurité doit être intégrée dans tous les domaines - appareils, applications et services de backend, qu'ils soient offerts directement ou par des tiers. Des tests réguliers et des mises à jour doivent être effectués pour minimiser les vulnérabilités.
- **Mises à jour -** informer les acheteurs de la possibilité de mise à jour des appareils et fournir ces mises à jour en toute sécurité avec une intervention ou un impact minimal de l'utilisateur (nécessitant une reconfiguration, par exemple).
- **Confidentialité -** divulguer clairement les politiques relatives à la confidentialité, telles que la collecte et le partage des données, et limiter la collecte à celle requise pour prendre en charge les fonctionnalités.
- **Divulgation -** des divulgations approfondies, facilement identifiables, couvrant les politiques de confidentialité, la collecte de données, les fonctionnalités avec ou sans connectivité et la durée du support / correctif permettent de prendre des décisions informées.
- **Contrôle -** les consommateurs ont le choix et le contrôle concernant les données collectées par le dispositif / service et la capacité de transférer ou d'effacer les données en cas de perte ou de vente.
- **Communications -** les communications avec les consommateurs après l'achat (par exemple, les informations de mise à jour / support) doivent être établies et sécurisées de manière proactive en utilisant les meilleurs pratiques pour limiter les attaques par ingénierie sociale.

Garantir des niveaux appropriés de sécurité et de confidentialité pour les produits et services IoT est une responsabilité collective. Les principes du cadre peuvent être utilisés par un large éventail de parties prenantes pour remplir leur rôle de protection des utilisateurs et d'Internet :

- **Les vendeurs d'IoT et leur chaîne d'approvisionnement -** En suivant ces principes, les fournisseurs peuvent accroître la confiance du marché dans les solutions IoT. Afin de sensibiliser et de mettre en évidence les leaders qui accordent la priorité à la sécurité et à la confidentialité des consommateurs, l'Internet Society demande aux fournisseurs de s'engager publiquement à respecter les principes du cadre.
- **Canaux de distribution (offres groupées, détaillants) -** Les principes du cadre peuvent être utilisés comme filtre pour déterminer les produits à transporter, assurant ainsi une meilleure sécurité et une plus grande confidentialité pour les acheteurs. L'Internet Society demande également que ces parties prenantes s'engagent publiquement à n'offrir que des produits qui soutiennent les principes du cadre.
- **Décideurs et agences gouvernementales -** L'Internet Society demande que les principes du cadre soient utilisés pour orienter les politiques, les lois et la réglementation associées aux produits et aux services IoT grand public afin de réduire les risques pour la sécurité et la confidentialité des consommateurs et des entreprises. Les gouvernements, en tant que grands acheteurs de solutions IoT, peuvent également utiliser le cadre comme base pour les besoins d'achat.

- **Organismes de test et d'examen des produits destinés aux consommateurs -** L'Internet Society demande que les principes du cadre soient intégrés dans les processus de test et d'examen. Cela sensibilisera les consommateurs dans leurs choix en matière de sécurité et de protection de confidentialité et favorisera de meilleures décisions d'achat.
- **Consommateurs et entreprises -** les consommateurs et les entreprises peuvent utiliser les principes du cadre comme guide pour faire des choix informés. Pour faciliter cela, l'Internet Society a fourni des listes de contrôle pour les consommateurs et les entreprises qui résument les principes clés.

En résumé, la commodité, l'efficacité et la perception promise des objets connectés sont menacées par des risques inutiles introduits par une sécurité et une confidentialité insuffisante dans la plupart des produits et services IoT d'aujourd'hui. Le cadre de confiance IoT de l'Internet Society identifie les exigences fondamentales que les fabricants, les fournisseurs de services, les distributeurs / acheteurs et les décideurs doivent comprendre, évaluer et adopter pour assurer la sécurité et la confidentialité dans le cadre des objets connectés.

0420-1