19 avril 2018

Sécurité de l'Internet des Objets (IdO) :

Briefing pour les décideurs politiques

« La cybersécurité sera le défi le plus pressant de la prochaine décennie, et l'IdO y jouera un rôle crucial. »

Rapport mondial sur l'Internet 2017 de l'Internet Society

Internet Society

Introduction

La nature ouverte de l'Internet crée la possibilité de connecter des appareils, des applications et des services backend à une ampleur qui transforme la façon dont nous interagissons avec notre environnement et notre société. L'Internet des Objets (IdO) a un énorme potentiel pour changer notre monde pour le mieux. Les projections relatives à l'impact de l'IdO sur l'économie mondiale sont impressionnantes, prévoyant une croissance explosive du nombre de dispositifs IdO et leur utilisation dans une grande variété de nouvelles applications passionnantes. Selon une estimation, « les appareils connectés seront au nombre de 38,5 milliards en 2020, contre 13,4 milliards en 2015 ».[1]

En même temps, avec des milliards d'appareils, d'applications et de services IdO déjà utilisés, et de plus en plus nombreux à venir en ligne, la sécurité de l'IdO est de la plus haute importance. Les appareils et services IdO mal sécurisés peuvent servir de points d'entrée pour les cyberattaques, compromettant les données sensibles et menaçant la sécurité des utilisateurs individuels. Les attaques contre les infrastructures et d'autres utilisateurs, alimentées par des réseaux de dispositifs IdO mal sécurisés, peuvent affecter la prestation de services essentiels tels que les soins de santé et les services publics de base, mettre en péril la sécurité et la vie privée d'autrui, et menacer la résilience de l'Internet dans le monde.

L'IdO présente également des défis importants en matière de protection des données. Ils seront abordés dans un document complémentaire sur la confidentialité et l'IdO.

Qu'est-ce que l'Internet des Objets (IdO) ? [2]

Le terme « Internet des Objets » se réfère aux **« scénarios où la connectivité réseau et la capacité informatique s'étendent aux objets, capteurs et articles du quotidien qui ne sont pas normalement considérés comme des ordinateurs, permettant à ces dispositifs de générer, échanger et consommer des données avec une intervention humaine minimale ».[3]** L'IdO comprend des produits de consommation, des biens durables, des voitures et des camions, des composants industriels et utilitaires, des capteurs, etc. Il présente aux utilisateurs une nouvelle façon d'interagir avec le réseau, en utilisant des périphériques qui ne sont pas limités aux ordinateurs traditionnels, smartphones et ordinateurs portables. L'IdO apporte de nouvelles opportunités inégalées pour les applications industrielles et les infrastructures critiques, mais aussi des défis significatifs. Bon nombre des défis et des recommandations abordés dans le présent document sont axés sur l'Internet des Objets à l'attention des consommateurs, mais s'appliquent également aux applications industrielles et d'infrastructure critique de l'IdO. Alors que les protocoles de communication locaux utilisés pour l'IdO, tels que Zigbee[4], LORA[5], Z-Wave[6] ou Bluetooth[7], présentent des défis intéressants, le principal objectif de l'Internet Society est de savoir comment les systèmes IdO interagissent avec, et affectent, l'Internet et ses utilisateurs.

1 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

2 Pour plus des ressources de la part de Internet Society concernant le sujet de l'IdO, visitez notre page d'accueil l'IdO (https://www.internetsociety.org/iot/), vous pouvez également consulter le document "The Internet of Things (IoT): An Overview"

3 https://www.internetsociety.org/doc/iot-overview

4 http://www.zigbee.org/what-is-zigbee/

5 https://www.lora-alliance.org/what-is-lora

6 http://www.z-wave.com/about

7 https://www.bluetooth.com/

Les appareils IdO compromis, tels que les webcams ou même les ampoules, peuvent être utilisés pour former des « réseaux de zombies », des réseaux de dispositifs contrôlés de l'extérieur connectés à Internet. Ces dispositifs, appelés dans ce contexte « botnets », sont souvent infectés par un logiciel malveillant et utilisés à des fins perturbatrices ou criminelles, telles que l'attaque d'autres réseaux, d'autres utilisateurs et de l'infrastructure Internet.[8] En 2016, un botnet d'appareils IdO compromis a effectué une attaque par déni de service distribué (DDoS) contre Dyn[9], un important fournisseur de services de système de noms de domaine (DNS). L'attaque a rendu les principaux sites Web, y compris Twitter, Amazon et Netflix, temporairement inaccessibles pour les utilisateurs d'Internet dans certaines régions du monde.

> À mesure qu'un plus grand nombre de dispositifs IdO vulnérables sont mis en ligne, ils créent une plus grande « surface d'attaque » et augmentent l'ampleur et la gravité potentielles des attaques DDoS basées sur l'IdO.

Comprendre l'impact croissant que la sécurité de l'IdO a sur l'Internet et ses utilisateurs est essentiel pour préserver l'avenir de l'Internet. Les fabricants d'IdO, les fournisseurs de services IdO, les utilisateurs, les organismes de standardisation, les décideurs et les régulateurs devront prendre des mesures pour se protéger des menaces à l'infrastructure Internet, telles que les attaques DDoS basées sur l'IdO. Il est également important de comprendre l'influence de la sécurité de l'IdO sur la confiance des utilisateurs et les pratiques en ligne.[10] La confiance est un ingrédient clé pour un Internet durable, évolutif et mondial. Sans confiance, les utilisateurs se sentent vulnérables et marginalisés et sont réticents à tirer parti des nombreux avantages légitimes qu'offre l'Internet. Parmi ceux qui se méfient de l'Internet, la principale raison est qu'ils croient que le réseau n'est pas sécurisé. [11] Cela étant dit, de nombreux utilisateurs de périphériques IdO peuvent ne pas se rendre compte qu'ils interagissent avec l'Internet. Construire un écosystème IdO sécurisé qui réduit les risques et protège contre les menaces tout en réalisant le vaste potentiel que l'IdO représente pour la société est crucial, urgent et doit être une priorité pour toutes les parties prenantes.

Il est plus important que jamais de relever les défis présentés par l'IdO selon une approche de sécurité collaborative[12]. À mesure que l'écosystème IdO se développe, le nombre d'appareils connectés potentiellement vulnérables augmente. Des périphériques vulnérables ne sont pas une fatalité. Aux côtés des acteurs individuels qui prennent leurs responsabilités dans leurs rôles respectifs, nous devons prendre ensemble des mesures pour réduire la probabilité que des appareils vulnérables soient produits, tout en réduisant l'impact des appareils vulnérables lorsqu'ils se retrouvent sur le réseau.

Les décideurs politiques ont des choix importants à faire pour aider à façonner l'avenir de la sécurité de l'IdO. Cet article est destiné aux régulateurs, aux décideurs et à toute personne intéressée par le développement et la mise en œuvre d'outils politiques concernant la sécurité de l'IdO.

8 https://www.internetsociety.org/policybriefs/botnets/

9 https://www.internetsociety.org/blog/2016/10/trust-isnt-easy-drawing-an-agenda-from-fridays-ddos-attack-and-the-internet-of-things/

10 https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/

11 https://www.cigionline.org/internet-survey

12 https://www.internetsociety.org/collaborativesecurity

Considérations principales

Il y a plusieurs facteurs à considérer dans l'approche de la sécurité de l'IdO. Parmi eux :

1. **L'IdO est un domaine en évolution et change rapidement et de manière organique.** De nouvelles fonctionnalités sont ajoutées et de nouvelles failles de sécurité sont découvertes presque tous les jours. Les meilleures pratiques et normes pour la sécurité de l'IdO sont encore émergentes et sont traitées par de nombreuses organisations à travers le monde.[13]

Le « **Cadre de Confiance pour l'IdO » de l'Online Trust Alliance (OTA) de l'Internet Society** est un ensemble complet de principes stratégiques aidant à sécuriser les appareils IdO et leurs données., du moment où ils sont produits et pendant toute leur durée de vie. Construit sur la base d'un processus collaboratif, ce cadre fournit des recommandations que tous les fabricants d'IdO devraient adopter pour améliorer la sécurité, la transparence et la communication de la capacité des dispositifs à être mis à jour, ainsi que les questions liées à la confidentialité des données.[14]

2. **L'IdO ne concerne pas seulement les appareils.** Les systèmes IdO sont interconnectés et complexes. Ils comprennent des logiciels, des dispositifs, des capteurs, des plate-formes et la transmission de données via Internet ainsi que les services comme l'analyse et le stockage de données dans le cloud (et potentiellement par des tiers). Étant donné que chaque partie d'un système IdO doit être sécurisée pour assurer la sécurité à ses utilisateurs et aux autres utilisateurs d'Internet, une approche par niveaux et en continu de la sécurité est requise.

3. **La sécurité intérieure et la sécurité extérieure sont distinctes mais tout aussi importantes**. Un système IdO peut être attaqué, affectant la vie privée et la sécurité de son utilisateur (p. ex. en exposant le flux vidéo « privé » d'un babyphone, en contrôlant les systèmes domestiques « intelligents », en provoquant un comportement indésirable (et potentiellement dangereux) des appareils ménagers, en les suivant lorsque les propriétaires sont absents) ; il s'agit d'un problème de « sécurité intérieure ». Mais un système IdO compromis peut également être utilisé pour lancer des attaques contre des tiers ou des systèmes (p. ex. des appareils ménagers vulnérables étant infectés par un « malware » (logiciel malveillant) et faisant partie d'un réseau botnet utilisé dans une attaque DDoS sur des réseaux, des utilisateurs ou une Infrastructure) ; il s'agit d'un problème de « sécurité extérieure ». Les systèmes IdO doivent être protégés contre les risques pour les autres réseaux et utilisateurs (sécurité extérieure) ainsi que les risques pour leurs utilisateurs et leurs biens (sécurité intérieure).

4. **La sécurité de l'IdO est une préoccupation mondiale.** L'Internet est un réseau de réseaux interconnecté et interdépendant et la sécurité d'une partie influence la sécurité de quiconque d'autre sur le réseau. Les systèmes IdO vulnérables peuvent être compromis de n'importe où et utilisés pour cibler n'importe qui.

13 https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/

14 The Online Trust Alliance (OTA) est une initiative de Internet Society. Consultez également les documents suivants: *Securing the Internet of Things et Internet of Things*, a *Vision for the Future.*
https://otalliance.org/iot
https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf
https://otalliance.org/system/files/files/initiative/documents/iot_visionforthefuture_0.pdf

5. **La sécurité par design est essentielle.** La sécurité de l'IdO est plus efficace quand elle est incluse dans le processus de conception depuis le début et tout au long de la mise en œuvre et le service après-vente. La sécurité ne peut pas être efficace lorsqu'elle est ajoutée après coup comme arrière-pensée.

6. **La sécurité est un processus continu.** Les systèmes IdO doivent être entretenus pour rester sécurisés. Actuellement, cette responsabilité incombe principalement aux fabricants IdO et aux fournisseurs de services. Des correctifs et des mises à jour rapides, vérifiables et efficaces pour corriger les vulnérabilités constituent un aspect essentiel de la sécurité. Les cycles de vie des produits et services sont un composant essentiel (p. ex. combien de temps le support et les mises à jour seront-ils disponibles, et que se passera-t-il une fois qu'ils auront cessé ?). Il n'est pas rare que les appareils restent en service longtemps après leur durée de vie annoncée.

7. **La recherche et les rapports sur les vulnérabilités sont importants.** Les chercheurs en sécurité jouent un rôle important en testant la sécurité des appareils et en alertant les fabricants et les fournisseurs de services sur la découverte de vulnérabilités.

8. **Les plates-formes sont des acteurs importants sur le marché.** Les plates-formes IdO (p. ex. Homekit d'Apple[15] et Weave de Google[16]) dont certaines ont une pénétration du marché considérable et croissante, permettent le contrôle d'une foule de dispositifs utilisant le même protocole, en échangeant des données pour prendre des décisions. Ceux qui ont été installés dans nos maisons « intelligentes », contrôlant la température, l'éclairage, les systèmes de son et la sécurité, utilisent des conceptions cohésives pour interagir facilement avec d'autres périphériques pris en charge et simplifier l'expérience utilisateur, dissimulant la complexité et l'ampleur de l'automatisation. Les caractéristiques de la plate-forme peuvent avoir un impact important sur le marché de l'Internet des Objets.[17] Les plates-formes avec de fortes exigences de sécurité poussent les fabricants et les fournisseurs partenaires à améliorer la sécurité de leurs périphériques et des services associés. Cependant, les vulnérabilités de la plate-forme peuvent affecter tous les systèmes de IdO connectés. En outre, les plates-formes varient dans leurs pratiques de protection des données, certaines étant meilleures que d'autres.

15 https://www.apple.com/ios/home/ ; https://developer.apple.com/homekit/

16 https://nest.com/weave/

17 https://www.internetsociety.org/blog/2017/09/can-iot-platforms-apple-google-samsung-make-home-automation-systems-secure/

Défis

En abordant la sécurité de l'IdO, il faut être conscient de nombreux défis. Entre autres :

- **L'économie favorise une sécurité faible.** Les pressions concurrentielles pour des délais de mise sur le marché plus courts et des produits moins chers incitent de nombreux concepteurs et fabricants de systèmes IdO, entre autres ceux qui produisent les dispositifs, les applications ou les services, à consacrer moins de temps et de ressources à la sécurité. Une sécurité élevée peut être coûteuse à concevoir et à mettre en œuvre, et prolonge le temps nécessaire de mise sur le marché d'un produit. La valeur commerciale des données utilisateur signifie également qu'il y a une incitation à accumuler le plus de données possibles le plus longtemps possible, ce qui va contre des bonnes pratiques de sécurité des données. En outre, il existe actuellement une pénurie de moyens crédibles et bien connus permettant aux fournisseurs de signaler leur niveau de sécurité aux consommateurs (p. ex. certifications et labels de confiance[18]). Il est donc difficile pour les consommateurs de comparer la sécurité des systèmes IdO concurrents, ce qui réduit les pressions des consommateurs pour une sécurité renforcée et fait qu'il est difficile pour les fournisseurs d'utiliser la sécurité comme un facteur de différenciation concurrentiel. De plus, le coût et l'impact d'une mauvaise sécurité tendent à tomber sur les consommateurs et les autres utilisateurs d'Internet, plutôt que sur les producteurs du système IdO vulnérable. Par exemple, si votre tuyauterie congèle lorsque le chauffage est coupé ou si les services Internet sont affectés par une attaque à laquelle participent vos appareils compromis, les effets ne sont pas directement ressentis par les producteurs.

- **La sécurité nécessite une expertise particulière.** La mise en œuvre d'une sécurité renforcée dans les systèmes IdO demande un savoir-faire. Les nouveaux acteurs de l'écosystème IdO peuvent avoir peu ou pas d'expérience en matière de sécurité Internet. Par exemple, un fabricant peut savoir comment rendre un réfrigérateur sécurisé pour son usage principal (câblage électrique, produits chimiques), mais peut ne pas comprendre les ramifications relatives à la sécurité d'Internet. Notamment, il peut ne pas comprendre l'impact global potentiel d'un système compromis dans un réfrigérateur « intelligent ».

- **Les systèmes IdO sont complexes et chaque partie doit être sécurisée.** Le niveau de sécurité d'un système est défini par le niveau de sécurité du maillon le plus faible. Dans les systèmes IdO, différents composants peuvent être sous le contrôle de différents acteurs dans différentes juridictions (p. ex. un serveur peut être situé dans un pays, alors que l'appareil peut être fabriqué dans un autre, et utilisé encore dans un autre), ce qui complique la résolution de manière coopérative des problèmes de sécurité liés à l'IdO et rend les défis de l'application transfrontalière particulièrement problématiques. Les chaînes d'approvisionnement complexes rendent les évaluations de sécurité difficiles, exigeant que les systèmes soient sécurisés de manière holistique avec une coordination entre les différentes personnes et les parties du système. De plus en plus, les systèmes IdO sont gérés et/ou contrôlés par (ou du moins, interagissent fortement) avec des services « cloud » gérés à distance, plutôt que d'être contrôlés localement. Le manque de transparence et de contrôle pour l'utilisateur final peut également être particulièrement problématique.

18 Une marque de confiance est un indicateur visible de la conformité à un ensemble bien conçu d'exigences de confiance, de sécurité, de confidentialité et/ou d'interopérabilité.

- **Le soutien à la sécurité doit être maintenu.** Les périphériques, applications et services IdO nécessitent généralement des correctifs et des mises à jour de sécurité pour se protéger contre les vulnérabilités connues. Les consommateurs n'ont généralement pas la capacité technique ou, dans de nombreux cas, même les interfaces utilisateur, d'implémenter efficacement et en toute sécurité les correctifs. Pour compliquer davantage les choses, lorsque le choix est disponible, les utilisateurs peuvent choisir de ne pas mettre à jour leurs appareils ou tout simplement ne pas savoir comment.[19] En outre, dans certains cas, les utilisateurs sont empêchés par contrat de mettre à jour ou de réparer les systèmes eux-mêmes ou de les faire réparer par des spécialistes indépendants, p. ex. le matériel agricole.[20] Malgré le fait que la prise en charge des systèmes IdO au fil du temps soit une tâche coûteuse et consommatrice de ressources pour les fournisseurs de services IdO et les développeurs, elle est souvent insuffisamment mise en priorité.

- **Les connaissances des consommateurs concernant la sécurité de l'IdO est faible.** En général, les consommateurs ont des connaissances limitées de la sécurité de l'IdO, ce qui a une incidence sur leur capacité à intégrer le facteur sécurité dans leurs habitudes d'achat ou à configurer et à entretenir la sécurité de leurs systèmes IdO. Les groupes et associations de consommateurs ont souvent des contraintes budgétaires, rendant la sensibilisation et la formation des consommateurs particulièrement difficiles.

- **Les incidents de sécurité peuvent être difficiles à détecter ou à résoudre par les utilisateurs.** Dans de nombreux cas, les effets d'un produit ou d'un système IdO mal sécurisé ne seront pas évidents pour l'utilisateur (p. ex. votre babyphone peut continuer à fonctionner comme un dispositif de surveillance audio et vidéo à distance, même après avoir été compromis et intégré à un réseau botnet effectuant des attaques DDoS ou avoir été modifié pour transmettre le son et les images à des parties non autorisées). Il est souvent difficile de détecter les fuites de données personnelles par les systèmes cloud IdO, en outre des nombreux appareils IdO manquent complètement d'interface utilisateur ou en ont une qui est sévèrement limitée. Dans ces cas (comme ci-dessus), il peut être difficile ou impossible pour un utilisateur d'interagir directement avec l'appareil pour confirmer ou effectuer des mises à jour, modifier la configuration, etc.

- **Les mécanismes de responsabilité légale existants peuvent être peu clairs**. La responsabilité pour les dommages causés par une sécurité inadéquate de l'IdO peut être difficile à déterminer. Cela entraîne de l'incertitude chez les victimes lorsqu'elles cherchent à attribuer une responsabilité ou à obtenir une indemnisation pour un préjudice. Une responsabilité claire peut être une incitation à renforcer la sécurité. En l'absence de régimes de responsabilité forts, les utilisateurs sont en fin de compte ceux qui paient le prix des atteintes à la sécurité.

19 Voir le processus multipartite du Département du commerce du NTIA des États-Unis ; évolutivité et correctif de sécurité de l'Internet des Objets (IdO). https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

20 https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

Recommandations et principes directeurs à l'intention des gouvernements sur la sécurité de l'Internet des Objets

Les gouvernements ont un rôle important à jouer dans la sécurisation de l'IdO. En utilisant leur formidable pouvoir de marché et en créant et mettant en œuvre avec soin des politiques et des réglementations, les gouvernements peuvent encourager un environnement plus sûr pour l'IdO. Les gouvernements détiennent un certain nombre de leviers importants qui, s'ils sont utilisés correctement, peuvent effectivement diriger l'industrie vers une autoréglementation efficace avec une responsabilisation claire et un partage d'information renforcé entre les fabricants d'IdO, les détaillants, les revendeurs, les intégrateurs, les fournisseurs de services et les consommateurs individuels. Une transparence accrue profite à toutes les parties prenantes.

Voici les principes directeurs et les recommandations que les gouvernements doivent prendre en compte lorsqu'ils traitent de la sécurité de l'Internet des Objets :

Renforcer la responsabilité

Principe : Renforcer la responsabilité relative à la sécurité et à la confidentialité de l'IdO en définissant des devoirs et des conséquences claires en cas de protection inadéquate.

Recommandations :

- **Assurer la sécurité juridique :** Fournir des règles claires, prévisibles et exécutables exigeant que les fournisseurs IdO, les développeurs et les fabricants se protègent contre les vulnérabilités connues en garantissant la mise en place de mécanismes de reporting, en mettant à jour leurs produits et systèmes avec des correctifs de sécurité, et en ayant des correctifs de sécurité et des politiques de mise à jour clairement définis, comprenant une date claire de fin de support. Surtout dans le marché de l'Internet des objets de consommation, les protections de sécurité devraient être intégrées par défaut (opt-out et non opt-in).

- **Renforcer la protection du consommateur :** Les données personnelles collectées ou utilisées par l'IdO, en particulier les données des capteurs, doivent être protégées par les lois sur la confidentialité et la protection des données. Les gouvernements peuvent améliorer la sécurité et la confidentialité en clarifiant comment les lois existantes sur la protection de la vie privée, la protection des données et la protection des consommateurs s'appliquent à l'IdO. À l'instar de l'interdiction des indications trompeuses sur la sécurité des produits, il faudrait également interdire aux entreprises de faire des déclarations trompeuses ou mensongères au sujet de leurs produits ou services IdO. Les détaillants devraient également partager la responsabilité et ne pas vendre des produits IdO présentant des défauts de sûreté et de sécurité critiques connus.

- **Attribuer clairement la responsabilité :** Pour faire face à l'incertitude, les gouvernements devraient clairement attribuer la responsabilité à ceux qui sont le plus en mesure d'exercer un contrôle sur le produit ou le service. Les fabricants et les importateurs de l'IdO devraient être responsables des défauts de sécurité et de sûreté de leurs produits.

Promouvoir l'utilisation de signaux de sécurité

Principe : Augmenter les incitations à investir dans la sécurité en favorisant un marché pour une évaluation indépendante et fiable de la sécurité de l'IdO.

Recommandations :[21]

- **Encourager des systèmes de certification de sécurité crédibles :** La certification, par laquelle une organisation signale qu'un produit ou un service a réussi un ensemble de tests de qualité ou de performance, peut constituer un signal de conformité puissant et visible pour savoir si un appareil IdO utilise les meilleures pratiques ou normes. Elle peut aussi être un outil efficace pour assigner et démontrer la responsabilité. (A noter que la conformité peut être autoévaluée ou validée à l'externe.) Améliorer la qualité des tests et des certifications, les considérer comme faisant partie d'un processus plutôt que comme un instantané et augmenter la visibilité des labels de confiance associés exercerait une pression sur les fabricants pour améliorer la sécurité et faire d'une meilleure sécurité un différenciateur compétitif.

- **Commentaires et évaluations :** Reconnaître le rôle utile que les évaluations et les critiques des consommateurs jouent en insistant sur les critères de confidentialité et de sécurité (ou leur absence) de l'IdO.

Encourager une culture de sécurité parmi les parties prenantes de l'IdO

Principe : Encourager la sécurité en tant que composante de toutes les étapes du cycle de vie du produit, y compris la conception, la production et le déploiement. Renforcer la capacité des parties prenantes à réagir et à atténuer les menaces basées sur l'IdO.

Recommandations *:*

- **Soutenir l'analyse des risques de sécurité :** Promouvoir l'utilisation de techniques d'évaluation des risques de sécurité acceptées par l'industrie avant que les produits et services IdO ne parviennent sur le marché. Encourager les fabricants et les fournisseurs IdO à utiliser des experts en sécurité indépendants pour entreprendre l'évaluation. Lorsque cela est possible, les gouvernements peuvent également soutenir le développement d'outils et de processus pour renforcer les analyses de risque (p. ex. en finançant la recherche). Ils peuvent travailler avec les organismes de financement gouvernementaux et l'industrie pour encourager la recherche accessible au public, y compris les mécanismes de sécurité et de politique.

21 "Systèmes" veut pas dire pas uniquement les systèmes IdO installés par l'utilisateur, mais aussi aux systèmes distants (ou "backend") impliqués dans la collecte, le stockage et le traitement des données. Ces systèmes peuvent ne pas être sous le contrôle des utilisateurs ou même dans leur juridiction.

- **Promouvoir les meilleures pratiques et les principes directeurs :** Promouvoir au niveau mondial l'utilisation de meilleures pratiques de sécurité fréquemment revues et communément admises et de principes directeurs pour guider la conception, le déploiement et l'utilisation des dispositifs et services IdO.[22] Inclure ces exigences dans les appels d'offres publics.

- **Encourager une culture de sécurité :** Favoriser une culture de sécurité parmi les principales parties prenantes, y compris les Fournisseurs d'accès Internet (FAI), qui va au-delà de leurs propres intérêts, pour couvrir l'Internet et ses utilisateurs. Par exemple, il est utile d'encourager le partage d'informations, y compris sur les techniques d'atténuation des menaces. En outre, fournir un soutien aux équipes de réponse aux incidents de sécurité informatique (CSIRT) et des ressources de formation et de référence en cybersécurité pour les nouveaux acteurs du marché de l'Internet des objets peut être très efficace.

- **Renforcer les protections juridiques pour les chercheurs en sécurité :** Veiller à ce que les chercheurs en sécurité ne courent aucun risque légal d'enquêter sur les vulnérabilités en matière de sécurité.

Fournir de fortes incitations pour de meilleures pratiques de sécurité

Principe : Les gouvernements peuvent utiliser leurs outils de politiques publiques et leur pouvoir de marché pour faire de la sécurité un facteur de différenciation concurrentiel.

Recommandations :

- **Améliorer les pratiques relatives aux appels d'offres publics pour l'IdO :** Développer des pratiques d'appels d'offres publics pour les dispositifs, plates-formes et services IdO qui mettent l'accent sur le respect des meilleures pratiques en matière de sécurité et de confidentialité. Lorsque les gouvernements génèrent un marché pour les meilleures pratiques en matière de sécurité de l'IdO, les entreprises réagissent pour répondre à la demande, influençant le marché public et privé de l'Internet des Objets. Si possible, les gouvernements devraient exiger que les fournisseurs IdO s'alignent avec des certifications ou labels de confiance de tiers dans le cadre des politiques d'appels d'offres. Les gouvernements devraient également utiliser les outils largement acceptés par l'industrie pour tester l'IdO dans leurs processus d'évaluation pour les appels d'offre.

- **Soutenir l'éducation des consommateurs :** Soutenir et engager des campagnes d'éducation et de sensibilisation des consommateurs pour stimuler la demande des consommateurs pour la sécurité de l'IdO. Lorsqu'une meilleure sécurité est perçue par les consommateurs comme un facteur de différenciation du marché, un argument crédible peut être présenté aux acheteurs potentiels selon lesquels des prix plus élevés sont justifiés.

- **Promouvoir un plus grand rôle pour les groupes de consommateurs :** Les groupes et association de consommateurs peuvent jouer un plus grand rôle dans le développement, la mise en œuvre, l'éducation du public et l'évaluation de la sécurité de l'Internet des Objets. (Actuellement, les groupes de consommateurs sont largement absents des discussions

22 Par exemple, le cadre de confiance IdO de l'OTA de l'Internet Society et la note d'information de l'Internet Society sur les invariants Internet.
https://otalliance.org/iot/
https://www.internetsociety.org/policybriefs/internetinvariants
Voir également les « Recommandations de sécurité de base pour l'Internet des Objets dans le contexte des infrastructures d'information critiques » de l'ENISA. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

pertinentes, ce qui contribue considérablement à l'ampleur du problème.) Reconnaître que le manque de financement empêche souvent les groupes de consommateurs de s'engager dans des discussions politiques relatives à la sécurité de l'IdO.

- **Collaborer avec l'industrie des assurances :** L'industrie des assurances peut prioriser de meilleures exigences en matière de confidentialité et de sécurité comme condition de souscription. En examinant la sécurité des appareils IdO et des applications et services connexes utilisés par les entreprises, les agences d'assurance peuvent prendre en compte le risque qu'ils présentent pour déterminer les primes et prix d'assurance.

Favoriser des solutions technologiquement neutres

Principe : Les solutions de sécurité ne doivent pas être basées sur des normes techniques spécifiques ou des produits commerciaux, mais plutôt sur des résultats souhaités tels qu'une meilleure sécurité, la confidentialité et l'interopérabilité. Ces objectifs ne changeront probablement pas fréquemment, mais les moyens de les atteindre changeront.

Recommandations :

- **Les politiques et les exigences d'appels d'offres publics pour la sécurité de l'IdO devraient spécifier les résultats, pas les méthodes :** Comme l'IdO évolue rapidement, de nouvelles menaces et de nouvelles méthodes et technologies de sécurité émergent constamment. En spécifiant les résultats plutôt que les technologies, les développeurs, les fabricants et les fournisseurs de services IdO sont libres d'innover. Cela permet de s'assurer que les politiques sont plus « à l'épreuve du futur » et n'auront pas besoin d'être modifiées de manière significative avec les nouvelles technologies. Un exemple de ceci serait les exigences relatives aux appels d'offres publics qui spécifient que les dispositifs, les applications et les services, devraient être régulièrement mis à jour, au besoin. Elles devraient également requérir une validation cryptographique de ces mises à jour et correctifs, et démontrer son efficacité, sans spécifier de moyens particuliers pour le faire.

- **Encourager la portabilité des données :** La prise en charge de normes ouvertes interopérables permet aux utilisateurs d'avoir plus de contrôle sur leurs données, car elles seront plus facilement transportables vers d'autres services. Les gouvernements ne devraient pas lier les données gouvernementales ou les données de leurs citoyens à des solutions propriétaires spécifiques, également connues sous le nom de « verrouillage des fournisseurs ».

Faire une utilisation intelligente des outils de politique publique et de réglementation

Principe : Comme la sécurité est coûteuse et que les utilisateurs peuvent avoir de la difficulté à reconnaître ou à évaluer la sécurité, les politiques publiques et les lois peuvent jouer un rôle important dans l'élaboration des pratiques de sécurité dans l'industrie de l'Internet des Objets. Des politiques publiques peuvent être élaborées dans le but d'influencer l'écosystème IdO pour promouvoir de meilleures pratiques de sécurité, plutôt que d'imposer des solutions techniques spécifiques.

Recommandations :

- **Les politiques publiques ou réglementations devraient être élaborées de manière transparente et mettre en priorité les intérêts des utilisateurs :** Pour renforcer les objectifs visés, toutes les parties prenantes affectées (y compris, mais sans s'y limiter, les fournisseurs, les fabricants, les utilisateurs et les organisations de consommateurs) devraient pouvoir contribuer à l'élaboration de politiques publiques et de lois. En représentant les intérêts des consommateurs, les organisations de consommateurs peuvent jouer un rôle très important dans l'élaboration des politiques publiques. Les décideurs devraient veiller à ce que les lois applicables à l'Internet des objets de consommation placent les intérêts des utilisateurs au premier plan. En outre, les effets des systèmes IdO non sécurisés sur d'autres utilisateurs du réseau, et pas seulement sur les utilisateurs directs, devraient être pris en compte dans l'élaboration des politiques publiques relatives à l'IdO.

- **La réglementation par secteur d'activité peut conduire à de meilleurs résultats :** Les principes fondamentaux, tels que la protection des données, devraient s'appliquer à tous les secteurs. Cependant, les systèmes IdO sont développés et utilisés dans un large éventail de secteurs et d'applications industriels ; par conséquent, une approche sectorielle de la réglementation, complémentaire aux principes fondamentaux, peut entraîner des résultats plus solides en matière de sécurité. Dans certains secteurs industriels, de fortes incitations du marché ou des réglementations existantes peuvent rendre la nouvelle réglementation moins nécessaire que dans d'autres. Par exemple, les outils réglementaires pouvant convenir au secteur des soins de santé peuvent ne pas être aussi utiles dans le secteur des appareils grand public, où des attributs comme la tolérance aux pannes peuvent ne pas être aussi cruciaux pour développer un produit sûr.

L'IdO est sur le point de transformer les économies et les sociétés du monde entier. La technologie apporte des opportunités énormes mais aussi des risques de même ampleur. Nous sommes à un moment critique où nous devons prendre des mesures pour faire en sorte que les avantages de l'Internet des Objets l'emportent sur les risques. De nombreuses organisations travaillent dur sur ces questions, mais toutes les parties prenantes, y compris les décideurs politiques, les fabricants et les consommateurs, doivent faire les bons choix quant à l'avenir de l'IdO et de sa sécurité.