Département américain de la sécurité intérieure

PRINCIPES STRATÉGIQUES POUR LA SÉCURISATION DE L'INTERNET DES CHOSES (IoT)

Version 1.0

15 novembre 2016

Homeland Security

La croissance des dispositifs, systèmes et services connectés en réseau, qui constituent l'internet des objets (IdO)[1], crée des opportunités et des avantages immenses pour notre société. Cependant, la sécurité de l'IdO n'a pas suivi le rythme rapide de l'innovation et du déploiement, créant des risques substantiels pour la sécurité et l'économie. Le présent document explique ces risques et fournit un ensemble de principes non contraignants et de meilleures pratiques suggérées afin de parvenir à un niveau de sécurité responsable pour les appareils et les systèmes que les entreprises conçoivent, fabriquent, possèdent et exploitent.

Croissance et prévalence de l'internet des objets

Les appareils connectés à l'internet permettent des connexions transparentes entre les personnes, les réseaux et les services physiques. Ces connexions permettent des gains d'efficacité, des utilisations inédites et des expériences personnalisées qui intéressent à la fois les fabricants et les consommateurs. Les appareils connectés au réseau sont déjà omniprésents, voire essentiels, dans de nombreux aspects de la vie quotidienne, qu'il s'agisse des trackers de fitness, des stimulateurs cardiaques, des voitures ou des systèmes de contrôle qui fournissent l'eau et l'électricité à nos foyers. Les promesses offertes par l'IdO sont presque illimitées.

Priorité à la sécurité de l'IdO

Si les avantages de l'IoT sont indéniables, la réalité est que la sécurité ne suit pas le rythme de l'innovation. Alors que nous intégrons de plus en plus de connexions réseau dans les infrastructures critiques de notre pays, des processus importants qui étaient autrefois exécutés manuellement (et bénéficiaient donc d'une certaine immunité contre les cyberactivités malveillantes) sont désormais vulnérables aux cybermenaces. Notre dépendance nationale croissante à l'égard des technologies connectées en réseau s'est accrue plus vite que les moyens de la sécuriser.

L'écosystème IoT présente des risques tels que la manipulation par des acteurs malveillants du flux d'informations en provenance et à destination des appareils connectés au réseau ou l'altération des appareils eux-mêmes, ce qui peut entraîner le vol de données sensibles et la perte de la vie privée des consommateurs, l'interruption des activités commerciales, le ralentissement des fonctionnalités de l'internet par des attaques par déni de service distribué à grande échelle et des perturbations potentielles des infrastructures critiques.

L'année dernière, lors d'une cyberattaque qui a temporairement mis hors service le réseau électrique de certaines régions d'Ukraine, le monde a pu constater les conséquences critiques que peuvent avoir les défaillances des systèmes connectés.
Parce que notre nation dépend désormais de réseaux fonctionnant correctement pour mener de nombreuses activités vitales, la sécurité de l'IdO est désormais une question de sécurité intérieure.

[1] Dans ce contexte, le terme IoT fait référence à la connexion de systèmes et de dispositifs à des fins essentiellement physiques (par exemple, détection, chauffage/refroidissement, éclairage, actionnement de moteurs, transport) à des réseaux d'information (y compris l'internet) via des protocoles interopérables, souvent intégrés dans des systèmes embarqués.

Il est impératif que le gouvernement et l'industrie travaillent ensemble, rapidement, pour s'assurer que l'écosystème IoT repose sur une base digne de confiance et sécurisée. En 2014, le comité consultatif du président sur les télécommunications de sécurité nationale (NSTAC) a souligné la nécessité d'une action urgente.

> L'adoption de l'IdO va augmenter à la fois en vitesse et en portée, et [aura] un impact sur pratiquement tous les secteurs de notre société. Le défi de la nation est de s'assurer que l'adoption de l'IdO ne crée pas de risques excessifs. En outre, il existe une petite fenêtre - qui se referme rapidement - pour s'assurer que l'IdO est adopté d'une manière qui maximise la sécurité et minimise les risques. Si le pays n'y parvient pas, il devra en assumer les conséquences pendant des générations. [2]

Le moment est venu de s'attaquer à la sécurité de l'IdO. Ce document pose les jalons d'un engagement avec les secteurs public et privé sur ces questions essentielles. Il s'agit d'une première étape pour motiver et encadrer les conversations sur les mesures positives pour la sécurité de l'IdO parmi les développeurs, les fabricants et les fournisseurs de services de l'IdO, ainsi que les utilisateurs qui achètent et déploient les appareils, les services et les systèmes. Les principes et pratiques suggérés ci-dessous permettent de mettre l'accent sur la sécurité et de renforcer le cadre de confiance qui sous-tend l'écosystème IoT.

Aperçu des principes stratégiques

De nombreuses vulnérabilités de l'IdO pourraient être atténuées grâce à des pratiques exemplaires reconnues en matière de sécurité, mais trop de produits aujourd'hui n'intègrent même pas de mesures de sécurité de base. De nombreux facteurs contribuent à ce manque de sécurité. L'un d'entre eux est le fait qu'il n'est pas toujours évident de déterminer qui est responsable des décisions en matière de sécurité dans un monde où une entreprise peut concevoir un appareil, une autre fournir les composants logiciels, une autre exploiter le réseau dans lequel l'appareil est intégré, et une autre déployer l'appareil. Ce défi est amplifié par l'absence de normes et de standards internationaux complets et largement adoptés pour la sécurité de l'IdO. Parmi les autres facteurs qui contribuent à cette situation, citons le manque d'incitations pour les développeurs à sécuriser correctement les produits, puisqu'ils ne supportent pas nécessairement les coûts d'un manquement à cette obligation, et une sensibilisation inégale à la manière d'évaluer les caractéristiques de sécurité des options concurrentes.

Les principes suivants, énoncés dans la section suivante, offrent aux parties prenantes un moyen d'organiser leur réflexion sur la manière de relever ces défis en matière de sécurité de l'IdO :

Intégrer la sécurité dès la phase de conception

Mises à jour de sécurité avancées et gestion des vulnérabilités

S'appuyer sur des pratiques de sécurité éprouvées

[2] Rapport du National Security Telecommunications Advisory Committee au président sur l'Internet des objets, 19 novembre 2014.

Prioriser les mesures de sécurité en fonction de leur impact potentiel

Promouvoir la transparence dans l'IdO

Connectez-vous prudemment et délibérément

Comme pour tous les efforts de cybersécurité, l'atténuation des risques liés à l'IdO est une responsabilité partagée entre le gouvernement et le secteur privé, qui évolue constamment. Les entreprises et les consommateurs sont généralement responsables de leurs propres décisions concernant les caractéristiques de sécurité des produits qu'ils fabriquent ou achètent. Le rôle du gouvernement, en dehors de certains contextes réglementaires spécifiques et des activités d'application de la loi, est de fournir des outils et des ressources pour que les entreprises, les consommateurs et les autres parties prenantes puissent prendre des décisions éclairées sur la sécurité de l'IdO.

Portée, objectif et public cible

L'objectif de ces principes non contraignants est de fournir aux parties prenantes des suggestions de pratiques qui les aident à prendre en compte la sécurité lorsqu'elles développent, fabriquent, mettent en œuvre ou utilisent des dispositifs connectés au réseau. Plus précisément, ces principes sont destinés à :

1	Les **développeurs de l'IdO** doivent tenir compte de la sécurité lors de la conception et du développement d'un dispositif, d'un capteur, d'un service ou de tout autre composant de l'IdO ;
2	Les **fabricants d'IoT** pour améliorer la sécurité des appareils des consommateurs et des appareils gérés par les fournisseurs ;
3	les **fournisseurs de services,** qui mettent en œuvre des services par le biais de dispositifs IoT, à prendre en compte la sécurité des fonctions offertes par ces dispositifs IoT, ainsi que la sécurité sous-jacente de l'infrastructure permettant ces services ; et
4	Les **consommateurs au niveau industriel et commercial** (y compris le gouvernement fédéral et les propriétaires et exploitants d'infrastructures critiques) pour servir de leaders dans l'engagement des fabricants et des fournisseurs de services sur la sécurité des appareils IoT.

Les principes énoncés ci-dessous sont conçus pour améliorer la sécurité de l'IdO dans l'ensemble des activités de conception, de fabrication et de déploiement. L'adoption généralisée de ces principes stratégiques et des pratiques suggérées associées améliorerait considérablement la sécurité de l'IdO. Il n'existe toutefois pas de solution unique pour atténuer les risques liés à la sécurité de l'IdO. Toutes les pratiques énumérées ci-dessous ne seront pas également pertinentes pour la diversité des dispositifs IoT. Ces principes sont destinés à être adaptés et appliqués par le biais d'une approche fondée sur les risques qui tient compte des contextes commerciaux pertinents, ainsi que des menaces et conséquences particulières pouvant résulter d'incidents impliquant un dispositif, un système ou un service connecté au réseau.

Intégrer la sécurité dès la phase de conception

La sécurité doit être évaluée comme une partie intégrante composante de tout appareil connecté au réseau. Bien qu'il y ait des exceptions, dans de trop nombreux cas, des facteurs économiques ou une méconnaissance des risques poussent les entreprises à commercialiser des appareils sans se soucier de leur sécurité. Intégrer la sécurité dès la phase de conception permet de réduire les perturbations potentielles et d'éviter l'effort beaucoup plus difficile et coûteux consistant à tenter d'ajouter la sécurité aux produits après leur développement et leur déploiement. En se concentrant sur la sécurité en tant que caractéristique des appareils connectés au réseau, les fabricants et les fournisseurs de services ont également la possibilité de se différencier sur le marché. Les pratiques ci-dessous sont quelques-unes des façons les plus efficaces de prendre en compte la sécurité dès les premières phases de conception, de développement et de production.

Quels sont les effets potentiels de l'absence de sécurité lors de la conception ?

Le fait de ne pas concevoir et mettre en œuvre des mesures de sécurité adéquates pourrait être préjudiciable au fabricant en termes de coûts financiers, de coûts de réputation ou de coûts de rappel du produit. Bien qu'il n'y ait pas encore de jurisprudence établie concernant le contexte de l'IdO, on peut s'attendre à ce que les principes traditionnels de la responsabilité civile des produits s'appliquent.

PRATIQUES SUGGÉRÉES :

Activez la sécurité par défaut grâce à des noms d'utilisateur et des mots de passe par défaut uniques et difficiles à craquer. Les noms d'utilisateur et les mots de passe des dispositifs IoT fournis par le fabricant sont les suivants

souvent jamais modifiés par l'utilisateur et sont facilement craqués. Les botnets fonctionnent en recherchant en permanence des dispositifs IoT protégés par des noms d'utilisateur et des mots de passe connus par défaut. Les contrôles de sécurité forts devraient être quelque chose que le consommateur industriel doit délibérément désactiver plutôt que d'activer délibérément.

Construisez l'appareil en utilisant le **système d'exploitation le** plus **récent** qui soit techniquement viable et économiquement réalisable. De nombreux dispositifs IoT utilisent des systèmes d'exploitation Linux, mais il se peut qu'ils n'utilisent pas le système d'exploitation le plus récent. L'utilisation du système d'exploitation actuel garantit que les vulnérabilités connues auront été atténuées.

Utilisez du **matériel qui intègre des fonctions de sécurité** pour renforcer la protection et l'intégrité du dispositif. Par exemple, utilisez des puces informatiques qui intègrent la sécurité au niveau des transistors, incorporées dans le processeur, et qui assurent le cryptage et l'anonymat.

Concevoir en tenant compte des perturbations du système et du fonctionnement. Comprendre les conséquences qui pourraient découler de la défaillance d'un dispositif permettra aux développeurs, aux fabricants et aux fournisseurs de services de prendre des décisions plus éclairées en matière de sécurité en fonction des risques. Dans la mesure du possible, les développeurs doivent construire des dispositifs IoT pour qu'ils tombent en panne de manière sûre et sécurisée, afin que la panne n'entraîne pas de perturbation systémique plus importante.

Promouvoir les mises à jour de sécurité a
et la gestion des vulnérabilités

Même lorsque la sécurité est prise en compte dès la phase de conception, des vulnérabilités peuvent être découvertes dans les produits après leur déploiement. Ces failles peuvent être atténuées par des correctifs, des mises à jour de sécurité et des stratégies de gestion des vulnérabilités. Lors de la conception de ces stratégies, les développeurs doivent prendre en compte les implications d'une défaillance du dispositif, la durabilité du produit associé et le coût anticipé de la réparation. En l'absence de la possibilité de déployer des mises à jour de sécurité, les fabricants peuvent être confrontés à la décision de faire des rappels coûteux ou de laisser en circulation des dispositifs présentant des vulnérabilités connues.

FOCUS ON : NTIA Multi-Processus des parties prenantes sur les correctifs et les mises à jour

L'Administration nationale des télécommunications et de l'information (NTIA) a convoqué un processus multipartite concernant la "mise à niveau et le correctif de l'Internet des objets" afin de réunir les parties prenantes pour partager les différents points de vue sur la mise à niveau et le correctif de sécurité, et pour établir des objectifs plus concrets en vue d'une adoption à l'échelle de l'industrie.

PRATIQUES SUGGÉRÉES :

Envisagez des moyens de **sécuriser le dispositif par des connexions réseau ou par des moyens automatisés**. Idéalement, les correctifs seraient appliqués automatiquement et s'appuieraient sur des protections cryptographiques d'intégrité et d'authenticité pour remédier plus rapidement aux vulnérabilités.

Envisagez de **coordonner les mises à jour logicielles entre les fournisseurs tiers** pour remédier aux vulnérabilités et aux améliorations de la sécurité afin de garantir que les appareils des consommateurs disposent de l'ensemble complet des protections actuelles.

Développer des **mécanismes automatisés pour traiter les vulnérabilités**. Dans le domaine de l'ingénierie logicielle, par exemple, il existe des mécanismes permettant d'ingérer en temps réel des informations provenant de rapports sur les vulnérabilités critiques émanant des communautés de chercheurs et de pirates informatiques. Cela permet aux développeurs de prendre en compte ces vulnérabilités dans la conception du logiciel et de réagir le cas échéant.

Élaborer une politique concernant la **divulgation coordonnée des vulnérabilités**, y compris les pratiques de sécurité associées pour traiter les vulnérabilités identifiées. Une politique de divulgation coordonnée doit impliquer les développeurs, les fabricants et les fournisseurs de services, et inclure des informations concernant toute vulnérabilité signalée à une équipe de réponse aux incidents de sécurité informatique (CSIRT). L'US Computer Emergency Readiness Team (US-CERT), l'Industrial Control Systems (ICS)-CERT et d'autres CSIRT fournissent régulièrement des alertes techniques, y compris après des incidents majeurs, qui donnent des informations sur les vulnérabilités et les mesures d'atténuation.

S'appuyer sur des pratiques de sécurité reconnues

De nombreuses pratiques éprouvées utilisées dans la sécurité informatique et réseau traditionnelle peuvent être appliquées à l'IdO. Ces approches peuvent aider à identifier les vulnérabilités, à détecter les irrégularités, à répondre aux incidents potentiels et à se remettre des dommages ou des perturbations subis par les dispositifs IoT.

FOCUS ON : Cadre de gestion des risques de cybersécurité du NIST

Le National Institute of Standards and Technology (NIST) a publié un cadre pour la gestion des risques liés à la cybersécurité qui a été largement adopté par le secteur privé, intégré entre les secteurs et au sein des organisations. Le cadre est largement reconnu comme une pierre de touche complète pour la gestion des risques cybernétiques des organisations https://www.nist.gov/cyberframework. Bien qu'il ne soit pas spécifique à l'IdO, le cadre de gestion des risques constitue un point de départ pour l'examen des risques et des meilleures pratiques.

PRATIQUES SUGGÉRÉES :

Commencez par les **pratiques de base en matière de sécurité logicielle et de cybersécurité** et appliquez-les à l'écosystème IoT de manière flexible, adaptative et innovante.

Se référer aux **directives sectorielles** pertinentes, lorsqu'elles existent, comme point de départ pour envisager les pratiques de sécurité. Certaines agences fédérales traitent des pratiques de sécurité pour les secteurs uniques qu'elles réglementent. Par exemple, la National Highway Traffic Safety Administration (NHTSA) a récemment publié des orientations sur les meilleures pratiques en matière de cybersécurité pour les véhicules modernes, qui abordent certains des risques uniques posés par les véhicules autonomes ou semi-autonomes. De même, la Food and Drug Administration a publié un projet d'orientation sur la gestion post-commercialisation de la cybersécurité desdispositifsmédicaux.

Pratiquez la défense en profondeur. Les développeurs et les fabricants doivent adopter une approche globale de la sécurité qui comprend des défenses en couches contre les menaces de cybersécurité, y compris les outils de niveau utilisateur en tant que points d'entrée potentiels pour les acteurs malveillants. Cela est particulièrement utile si les mécanismes de correction ou de mise à jour ne sont pas disponibles ou insuffisants pour remédier à une vulnérabilité spécifique.

Participer à des **plates-formes de partage d'informations** pour signaler les vulnérabilités et recevoir en temps utile des informations essentielles sur les cybermenaces et les vulnérabilités actuelles des partenaires publics et privés. Le partage d'informations est un outil essentiel pour garantir que les parties prenantes sont au courant des menaces dès qu'elles se présentent3. Le National Cybersecurity and Communications Integration Center (NCCIC) du Department of Homeland Security (DHS), ainsi que les centres de partage et d'analyse d'informations (ISAC) et les organisations de partage et d'analyse d'informations (ISAO) multi-états et sectoriels, en sont des exemples.

[3] "Information Sharing", National Cybersecurity and Communications Information Center.

Prioriser les mesures de sécurité en fonction de leur impact potentiel

Les modèles de risque diffèrent considérablement dans l'écosystème IoT. Par exemple, les consommateurs industriels (tels que les propriétaires et exploitants de réacteurs nucléaires) auront des considérations différentes de celles d'un consommateur de détail. Les conséquences d'une défaillance de la sécurité chez les différents clients varieront également de manière significative.
Il est donc essentiel de se concentrer sur les conséquences potentielles d'une perturbation, d'une violation ou d'une activité malveillante sur l'ensemble des consommateurs afin de déterminer où il convient d'orienter les efforts de sécurité et qui est le mieux à même d'atténuer les conséquences importantes.

Les mesures de sécurité de l'IdO doivent-elles se concentrer sur le dispositif IdO ?

Étant donné que l'objectif de tous les processus IoT est de recueillir des informations à un point physique et de motiver une décision basée sur ces informations (avec parfois des conséquences physiques), les mesures de sécurité peuvent se concentrer sur une ou plusieurs parties du processus IoT. Comme indiqué précédemment, les risques liés à l'IdO commencent avec le dispositif spécifique, mais ne s'y limitent certainement pas. Les développeurs, les fabricants et les fournisseurs de services doivent prendre en compte les risques spécifiques à l'appareil IoT ainsi qu'au processus et au service, et décider, en fonction de l'impact relatif sur les trois, où les mesures les plus robustes doivent être appliquées.

PRATIQUES SUGGÉRÉES :

Connaître l'**utilisation et l'environnement prévus d'**un appareil, dans la mesure du possible. Cette prise de conscience aide les développeurs et les fabricants à prendre en compte les caractéristiques techniques de l'appareil IoT, la façon dont l'appareil peut fonctionner et les mesures de sécurité qui peuvent être nécessaires.

Effectuez un **exercice de** "**red-teaming"**, dans lequel les développeurs tentent activement de contourner les mesures de sécurité nécessaires au niveau des applications, du réseau, des données ou des couches physiques. L'analyse et la planification des mesures d'atténuation qui en résultent devraient permettre de hiérarchiser les décisions sur le lieu et la manière d'intégrer des mesures de sécurité supplémentaires.

Identifier et authentifier les dispositifs connectés au réseau, notamment pour les consommateurs industriels et les réseaux d'entreprise. L'application de mesures d'authentification pour les dispositifs et services connus permet au consommateur industriel de contrôler les dispositifs et services qui se trouvent dans son cadre organisationnel.

Promouvoir la transparence dans l'IdO

Dans la mesure du possible, les développeurs et les fabricants doivent connaître leur chaîne d'approvisionnement**,** à savoir s'il existe des vulnérabilités associées aux composants logiciels et matériels fournis par des fournisseurs extérieurs à leur organisation. La dépendance à l'égard des nombreuses solutions logicielles et matérielles peu coûteuses et facilement accessibles utilisées dans l'IdO peut rendre cette tâche difficile. Étant donné que les développeurs et les fabricants s'appuient sur des sources extérieures pour obtenir des solutions logicielles et matérielles peu coûteuses et facilement accessibles, ils peuvent ne pas être en mesure d'évaluer avec précision le niveau de sécurité intégré dans les composants lors du développement et du déploiement de dispositifs connectés au réseau. En outre, étant donné que de nombreux dispositifs IoT s'appuient sur des paquets open source, les développeurs et les fabricants ne sont souvent pas en mesure d'identifier les sources de ces composants.

Une sensibilisation accrue pourrait aider les fabricants et les consommateurs industriels à déterminer où et comment appliquer des mesures de sécurité ou intégrer des redondances. En fonction du profil de risque du produit en question, les développeurs, les fabricants et les prestataires de services seront mieux équipés pour atténuer les menaces et les vulnérabilités de manière appropriée et aussi rapidement que possible, que ce soit par l'application de correctifs, le rappel du produit ou la mise en garde des consommateurs.

PRATIQUES SUGGÉRÉES :
Effectuez des évaluations des risques de bout en bout qui tiennent compte des **risques** internes et des **risques liés aux fournisseurs tiers,** dans la mesure du possible. Les développeurs et les fabricants devraient inclure les vendeurs et les fournisseurs dans le processus d'évaluation des risques, ce qui créera de la transparence et leur permettra de prendre conscience des vulnérabilités potentielles des tiers et de promouvoir la confiance et la transparence. La sécurité doit être réévaluée en permanence à mesure que le composant de la chaîne d'approvisionnement est remplacé, retiré ou mis à niveau.
Envisagez de créer un **mécanisme divulgué publiquement pour utiliser les rapports de vulnérabilité**. Les programmes Bug Bounty, par exemple, s'appuient sur des méthodes de crowdsourcing pour identifier les vulnérabilités que les équipes de sécurité internes des entreprises ne peuvent pas toujours détecter.
Envisager le développement et l'utilisation d'une nomenclature **logicielle** pouvant être utilisée comme moyen d'instaurer une confiance partagée entre les vendeurs et les fabricants. Les développeurs et les fabricants devraient envisager de fournir une liste des composants matériels et logiciels connus dans l'emballage de l'appareil d'une manière qui tienne compte de la nécessité de protéger les questions de propriété intellectuelle. Cette liste peut être un outil précieux pour les autres acteurs de l'écosystème IoT, qui pourront ainsi comprendre et gérer leurs risques et corriger les vulnérabilités immédiatement après un incident.

Connectez-vous prudemment et délibérément

Les consommateurs d'IoT, en particulier dans le contexte industriel, doivent délibérément se demander si une connectivité continue est nécessaire compte tenu de l'utilisation du dispositif IoT et des risques associés à sa perturbation. Les consommateurs IoT peuvent également contribuer à contenir les menaces potentielles posées par la connectivité du réseau en se connectant avec précaution et de manière délibérée, et en mettant en balance les risques d'une violation ou d'une défaillance potentielle d'un dispositif IoT avec les coûts de la limitation de la connectivité à Internet.

Dans l'environnement en réseau actuel, il est probable que tout dispositif IoT donné puisse être perturbé au cours de son cycle de vie. Les développeurs, les fabricants et les consommateurs de dispositifs IoT doivent tenir compte de l'impact d'une perturbation sur la fonction principale du dispositif IoT et sur les opérations commerciales qui suivent la perturbation.

Chaque appareil en réseau doit-il être connecté en permanence et automatiquement à l'Internet ?

En 2015, la Federal Trade Commission a publié un guide intitulé "Start with Security : A Guide for Businesses" pour les aider à déterminer cette même question. S'il peut être pratique d'avoir un accès continu au réseau, cela peut ne pas être nécessaire pour l'objectif de l'appareil - et des systèmes ; par exemple, les réacteurs nucléaires, où une connexion continue à Internet ouvre la possibilité d'une intrusion aux conséquences potentiellement énormes.

PRATIQUES SUGGÉRÉES :

Informer les consommateurs d'appareils IdO de l'usage prévu de toute connexion réseau. Les connexions internet directes peuvent ne pas être nécessaires pour faire fonctionner les fonctions critiques d'un dispositif IoT, en particulier dans le cadre industriel. Les informations sur la nature et l'objectif des connexions peuvent éclairer les décisions des consommateurs.

Établissez des connexions intentionnelles. Dans certains cas, il est dans l'intérêt du consommateur de ne pas se connecter directement à l'Internet, mais plutôt à un réseau local qui peut regrouper et évaluer toute information critique. Par exemple, les systèmes de contrôle industriel (ICS) doivent être protégés par les principes de défense en profondeur publiés par https://ics- cert.us-cert.gov/recommended_practices.

Intégrer des contrôles pour permettre aux fabricants, aux fournisseurs de services et aux consommateurs de désactiver des connexions réseau ou des ports spécifiques lorsque cela est nécessaire ou souhaité pour permettre une **connectivité sélective**. En fonction de l'objectif de l'appareil IoT, fournir aux consommateurs des conseils et un contrôle sur la mise en œuvre finale peut être une bonne pratique.

CONCLUSION

Notre nation ne peut pas se permettre une génération de dispositifs IoT déployés avec peu de considération pour la sécurité. Les conséquences sont trop importantes compte tenu du potentiel de nuisance pour nos infrastructures critiques, notre vie privée et notre économie.

Au moment où le DHS publie ces principes, nous reconnaissons les efforts en cours de nos collègues des autres agences fédérales, ainsi que le travail des entités du secteur privé pour faire progresser les architectures et instituer des pratiques visant à assurer la sécurité de l'IdO. Ce document est une première étape pour renforcer ces efforts en articulant des principes de sécurité globaux. Mais d'autres étapes seront certainement nécessaires.

Le DHS identifie quatre lignes d'effort qui devraient être entreprises par le gouvernement et l'industrie pour renforcer la sécurité de l'IdO.

QUATRE LIGNES D'EFFORT :
Coordonner l'ensemble des départements et agences fédéraux pour s'engager auprès des parties prenantes de l'IdO et explorer conjointement les moyens d'atténuer les risques posés par l'IdO. Le DHS et ses partenaires fédéraux continueront à s'engager auprès des partenaires industriels pour déterminer les approches susceptibles d'améliorer la sécurité de l'IdO, et pour promouvoir la compréhension des tendances technologiques en évolution qui peuvent traiter les risques de l'IdO. Les efforts futurs porteront également sur la mise à jour et l'application de ces principes, à mesure que les meilleures pratiques et approches seront affinées et comprises.
Sensibiliser les parties prenantes aux risques liés à l'IdO. Il est important que les parties prenantes soient conscientes des risques liés à l'IdO afin qu'elles puissent se positionner pour y faire face. Le DHS va accélérer les initiatives de sensibilisation, d'éducation et de formation du public, en partenariat avec d'autres agences, le secteur privé et des partenaires internationaux. Le DHS, en collaboration avec d'autres agences, entreprendra également des initiatives plus directement adaptées à des secteurs particuliers et à des consommateurs individuels.
Identifier et faire progresser les incitations à l'intégration de la sécurité de l'IdO. Les décideurs, les législateurs et les parties prenantes doivent envisager des moyens de mieux encourager les efforts visant à renforcer la sécurité de l'IdO. Dans l'environnement actuel, il est trop souvent difficile de déterminer qui est responsable de la sécurité d'un produit ou d'un système donné. En outre, les coûts d'une sécurité insuffisante ne sont souvent pas supportés par ceux qui sont les mieux placés pour améliorer la sécurité. Le DHS et toutes les autres parties prenantes doivent examiner comment la responsabilité civile, la cyberassurance, la législation, la réglementation, la gestion de la certification volontaire, les initiatives de normalisation, les initiatives volontaires au niveau de l'industrie et d'autres mécanismes pourraient améliorer la sécurité tout en encourageant l'activité économique et l'innovation révolutionnaire. À l'avenir, le DHS se réunira avec ses partenaires pour discuter de ces questions essentielles et solliciter des idées et des commentaires.
Contribuer aux processus d'élaboration de normes internationales pour l'IdO. L'IdO fait partie d'un écosystème mondial, et d'autres pays et organisations internationales commencent à évaluer bon nombre de ces mêmes considérations de sécurité. Il est important que les activités liées à l'IdO ne se divisent pas en ensembles de normes ou de règles incohérentes. Alors que le DHS se concentre de plus en plus sur les efforts liés à l'IdO, nous devons nous engager avec nos partenaires internationaux et le secteur privé pour soutenir le développement de normes internationales et veiller à ce qu'elles soient conformes à notre engagement à encourager l'innovation et à promouvoir la sécurité.

Le DHS se réjouit de ces prochaines étapes de collaboration. Ensemble, nous pouvons, et devons, relever ces défis complexes. Ce faisant, nous ferons en sorte que l'avenir de notre réseau connecté soit non seulement innovant, mais aussi sécurisé et construit pour durer.

EN ANNEXE : CONSEILS ET RESSOURCES SUPPLÉMENTAIRES

Les principes contenus dans ce document ont été élaborés sur la base des informations recueillies dans les rapports de l'industrie et lors de discussions avec le secteur privé, les associations professionnelles, les entités non gouvernementales et les partenaires fédéraux, notamment le NIST et le NTIA.

Département de la sécurité intérieure

- https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf
- https://www.dhs.gov/publication/security-tenets-lces
- https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

Autres entités fédérales

- Comité consultatif sur les télécommunications pour la sécurité nationale
    1. Rapport final du NSTAC sur l'Internet des objets

- NTIA
    1. Avis et demande de commentaires sur les avantages, les défis et les rôles potentiels du gouvernement dans la promotion de l'Internet des objets rôles potentiels du gouvernement pour favoriser l'avancement de l'Internet des objets
        a) Commentaires
    2. Livre vert - Cybersécurité, innovation et économie de l'internet, 2011
    3. De nouvelles perspectives pour l'Internet des objets émergent
    4. Remarques de la secrétaire adjointe adjointe Simpson lors de l'atelier " Fostering the Advancement " (favoriser l'avancement) de l'Internet des objets, 9/9/2016
        a) Annonce de l'atelier sur la promotion de l'Internet des objets
    5. Ressource/examen/catalogue de l'Internet Policy Task Force sur les avantages, les défis et les rôles potentiels du gouvernement pour favoriser l'avancement de l'Internet des objets.

- NIST
    1. Cadre de cybersécurité
    2. Programme Systèmes cyber-physiques (CPS)
        a) Projet de groupe de travail public (PWG) sur les systèmes cyber-physiques(CPS) Framework version 1.0
            - Commentaires acceptés jusqu'au2 septembre 2015

3. Programme Smart-Grid
4. Groupe de travail technique international sur le cadre desvilles intelligentes basées sur l'IdO (International Technical Working Group on IoT-Enabled Smart CityFramework)
5. Publication spéciale (SP) 800-183 du NIST, Réseau des objets, 28/07/2016.
    a) Communiqué de presse du NIST

- Commission fédérale du commerce
    1. Rapport du personnel de la FTC, "Internet of Things : Privacy & Security in a Connected World ", janvier 2015.

- Congrès des États-Unis
    1. Audience de la commission du Sénat sur le commerce, les sciences et les transports, "Le monde connecté : Examen de l'Internet desobjets".
    2. Résolution unanimement bipartisane du Sénat (S. Res. 110) appelant à une stratégie nationale pour guider le développement de l'Internet des objets.
    3. Commission de l'énergie et du commerce de la Chambre des représentants, "L'Internet des objets : Explorer la prochainefrontièretechnologique"
- Government Accounting Office
    1. Engagement du GAO avec le DHS : le GAO est actuellement engagé avec le DHS sur l'IdO, code 100435 [lettre de notification du 15 janvier 2016 disponible via ce lien].
        a) Statut/entrée dans la liste la plus récente, celle du 3 juin 2016, des missions actives du GAO liées auDHS.

Sources externes

La liste des ressources supplémentaires est fournie uniquement à titre de référence et ne constitue pas une approbation par le ministère de la Sécurité intérieure (DHS). Le DHS ne cautionne aucun produit, service ou entreprise commerciale.

- Conseil atlantique
    1. Les maisons intelligentes et l'internet des objets - http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
- Je suis la cavalerie
    1. Cadre de cybersécurité automobile à cinq étoiles - https://iamthecavalry.org/5star
    2. Serment d'Hippocrate pour les dispositifs médicaux connectés - https://iamthecavalry.org/oath
- Alliance pour la confiance en ligne
    1. Meilleures pratiques pour les consommateurs

- Industrial Internet Consortium : http://www.iiconsortium.org/IISF.htm
- Projet ouvert de sécurité des applications Web (OWASP)
    1. Projet Internet des objets
       https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
    2. Guide de la sécurité de l'Internet des objets
       https://www.owasp.org/index.php/IoT_Security_Guidance
- Safecode.org meilleures pratiques industrielles pertinentes www.safecode.org
- AT&T
    1. Explorer la sécurité de l'IdO
- Symantec
    1. Architecture de référence de l'Internet des objets
       https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-fr.pdf