LES DOSSIERS TECHNIQUES

Sécurité de l'Internet des Objets

Introduction aux principaux risques et approches de sécurisation

Juin 2022

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Bertrand	**CARLIER**	Wavestone

Les contributeurs :

Sami	**CHAMAM**	Brightway
Louis-Henry	**DUPETY**	Holiseum
Bruno	**GUIOT**	EDF
Stéphanie	**JOUVE**	Médiane Système
Thierry	**MATUSIAK**	Microsoft
Thomas	**MERLY**	Eliade

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Ce document a pour objet de présenter les principaux risques relatifs spécifiquement à un objet connecté ou à son écosystème. Il fournit également des premières pistes de points de contrôle et de mesures de sécurité adaptées au monde des objets connectés et qui sont d'ores et déjà considérées comme de bonnes pratiques.

Il s'adresse tout autant aux Responsables de la Sécurité du Système d'Information (RSSI) et à leur équipe qu'aux acteurs métiers ou projets amenés à manipuler ces objets connectés.

Le sujet sera principalement abordé selon le point de vue d'une entreprise utilisatrice intégrant un ou plusieurs objets connectés dans ses processus. Cependant les conseils prodigués dans ce document pourront tout autant être de précieuses sources d'informations pour tout concepteur ou fabricant d'objet connecté.

Chaque risque, illustré par des scénarios d'attaque - soit connus et publics, soit réalistes dans un contexte d'entreprise - sera détaillé en termes de conséquences et donc d'impacts. Des premières pistes de sécurisation de l'objet connecté et de son écosystème seront fournies.

Des mesures de protection et des points de contrôles adaptés à la plupart des projets IoT seront ensuite présentés avec les points clés à aborder pour permettre d'en assurer l'efficacité.

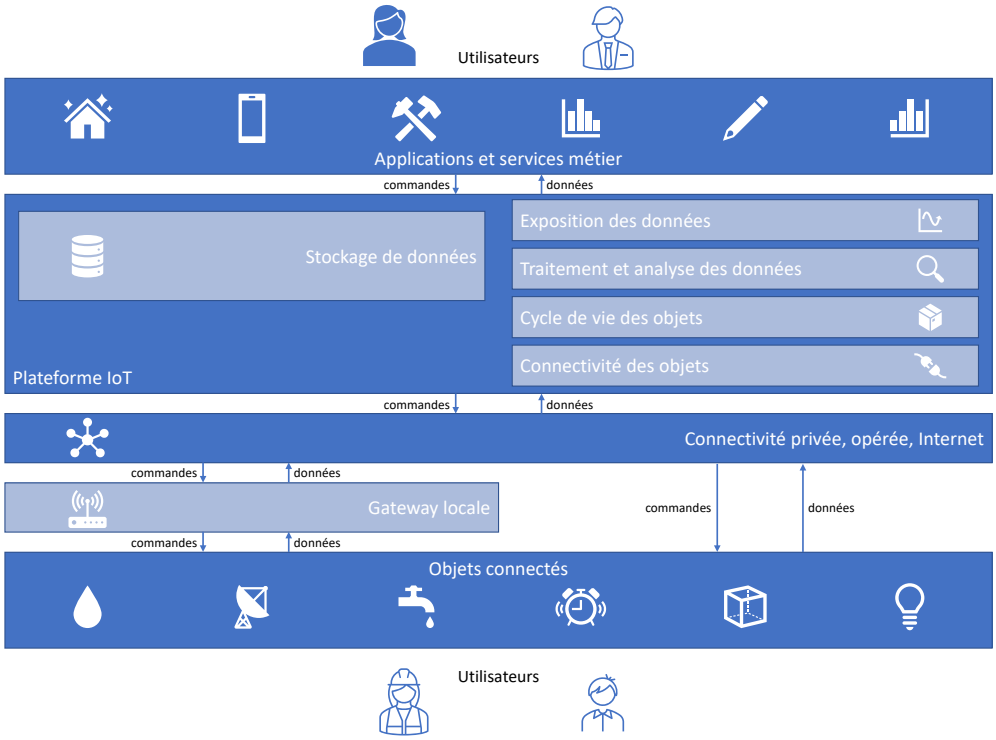
Enfin, nous présenterons de manière synthétique comment ces différentes mesures de sécurité contribuent à couvrir l'ensemble des risques présentés.

Dans la mesure du possible, nous essayons ici de considérer à la fois les objets connectés (IoT) et l'informatique industrielle (OT).

1.1 Présentation de l'objet et son écosystème

Une solution IoT repose généralement sur 3 piliers :

- L'objet lui-même
- L'infrastructure à laquelle il est connecté
- Les utilisateurs interagissant directement ou indirectement avec l'objet



À la base de la solution IoT : l'objet lui-même

Il est générateur de données via ses capteurs et récepteurs de commandes et d'actions qui lui sont envoyées. Il est déployé potentiellement massivement, sous des modalités très diverses :

- Un objet complexe et autonome,
- Un capteur extrêmement contraint associé à un équipement existant,
- Un objet déployé en proximité d'une source d'alimentation ou de connectivité
- Un objet déployé au contraire dans un environnement isolé, etc.

Connecté à l'objet : l'infrastructure

Les objets s'insèrent ensuite dans un "écosystème", conçu pour absorber et traiter les flux de données. Cette infrastructure, régulièrement appelée « plateforme IoT », peut assurer plusieurs fonctions :

- Authentification des objets,
- Connectivités protocolaire et applicative,
- Manipulation des données et interaction avec des applications du SI traditionnel,
- Gestion de la flotte d'objets (mise à jour, ajout, révocation, etc.)

De nombreux fournisseurs de plateformes sont présents sur le marché, essentiellement en mode SaaS, des plus généralistes (AWS, Microsoft, Google, IBM, etc.) aux plus spécialisés sur certaines verticales et industries (PTC ThingWorx, Siemens, Bosch, Schneider Electric, etc.) en passant par des fournisseurs de plateformes managées (Accenture, CapGemini, etc.) ou des opérateurs de télécommunication (Objenious, T-Mobile, AT&T, etc.)

Interagissant avec l'objet : les utilisateurs

Enfin, il ne faut pas oublier le grand nombre d'utilisateurs qui peut manipuler ou interagir avec les objets : utilisateurs finaux (clients ou employés), mainteneurs se déplaçant sur le terrain ou bien supervisant à distance, chargés de relation client ou personnel du service support à même de dépanner les utilisateurs finaux, etc.

La grande diversité d'objets, le nombre d'interfaces important, l'hétérogénéité des plateformes sur lesquelles nous avons un contrôle limité, la multitude d'acteurs impliqués de la conception à l'utilisation en passant par la fabrication et la distribution, entre autres, font de la gestion de la cybersécurité de ces écosystèmes un casse-tête extrêmement complexe.

1.2 Impact organisationnel en entreprise

Notre constat initial est que les objets connectés peuvent impacter tout l'écosystème de sécurité en place dans les entreprises. De plus, on ne peut pas sécuriser ce que l'on ne connait pas. Pour prendre en compte les risques spécifiques à l'IoT, les équipes "**sécurité**" ont besoin d'avoir connaissance des projets IoT en cours, grâce à des échanges réguliers avec les équipes "**conception**" et "**innovation**" concernées. Ces échanges peuvent probablement être initiés au travers d'une étape de sensibilisation.

L'analyse des risques peut alors être initiée avec l'équipe "**risques**". Elle peut inclure une évaluation du niveau de sécurité des fournisseurs d'objets ou de leurs composants, au moins au travers des labels et certifications dont ils disposent. En pratique, il s'agit ensuite de définir des scénarios d'attaque incluant les objets et leur détournement potentiel.

L'équipe "**gestion des Vulnérabilités**" peut aussi inclure les objets déployés dans ses analyses régulières, pour identifier les vulnérabilités et configurations faibles. Les outils d'analyse (scanners) doivent donc supporter ces nouveaux terminaux. Si nécessaire,

l'entreprise pourra compléter son arsenal de scanners par une solution spécialisée, et faire appel à une équipe "**tests d'intrusion**" spécialisée. L'importance et le niveau de gravité des vulnérabilités identifiées dépendent également étroitement de la spécificité des objets et de leur écosystème (localisation physique, options de configuration, score CVSS[1], faisabilité de l'attaque, activité réelle dans les systèmes de l'entreprise, criticité des points concernés, évènements redoutés, tolérance au risque de l'entreprise et obligations de conformité).

La collaboration avec le "**responsable métier**" doit permettre d'identifier et de gérer les priorités. La remédiation passe souvent par, dans un premier temps, une qualification "humaine" du meilleur plan d'action à implémenter, quel que soit son niveau :

- Documentation d'exceptions (réévaluées régulièrement)
- Supervision des vulnérabilités connues
- Contremesures (isolation réseau, fermeture de ports...)
- Suppression de vulnérabilité(s) (solution privilégiée quand elle est raisonnable en termes de coût ou d'impact)

Dans un second temps, par la vérification des actions menées, la validation de leur efficacité, et le suivi de la non-régression au fil du temps.

L'IoT a aussi un impact sur les activités de "**surveillance de la menace**". Le CERT / CSIRT réalise une veille technologique régulière, qu'il faut compléter avec un volet spécifique IoT, en surveillant par exemple l'exploitation des vulnérabilités auxquelles l'entreprise se sait exposée. Une importance particulière doit être portée à l'analyse *post mortem* des premiers incidents propres à l'IoT auxquels l'entreprise pourrait être exposée par la suite, pour améliorer les processus mis en place initialement.

La surveillance des objets concerne bien sûr le "**SOC**[2]", qu'il soit unique et centralisé ou qu'il soit dédié aux objets connectés (par exemple pour la surveillance d'une flotte de véhicules connectés), qui doit donc connaitre leur empreinte sur le réseau et développer des scénarios de détection spécifiques (et/ou étendre les scénarios existants). La décision de déployer un SOC dédié peut être pertinente dans certains cas, par exemple pour un fournisseur d'objets, afin d'en assurer la sécurité auprès de ses clients.

L'équipe "**réponse à incidents**" définit également des procédures (*Playbooks*) spécialisées (et/ou complète les procédures existantes), là aussi pour tenir compte des spécificités du domaine IoT (point sur lequel on reviendra dans le reste de ce document).

En phase de "**production**", les mises à jour sont régulières, parfois fonctionnelles, parfois techniques. Elles doivent être le plus automatique possible, surtout pour les objets autonomes, mais effectuées par un mécanisme sécurisé et par du personnel autorisé (cf. ISO 27402).

Il faut également bien garder en tête que ce maintien en conditions de sécurité (MCS) des objets dans le temps est un élément majeur impactant l'organisation habituelle. C'est d'autant plus important que de nombreux objets ont un "**environnement d'exécution**" sur lequel l'entreprise a peu ou pas de contrôle. Un capteur peut par exemple se trouver dans un lieu public, directement accessible, et donc exposé à des attaques ou des compromissions "physiques". Enfin, les "**utilisateurs**" ont aussi un rôle à jouer dans cet écosystème, en prenant conscience des nouveaux enjeux de sécurité inhérents aux objets connectés. Cela peut passer par une extension des programmes de sensibilisation en place.

On le voit : c'est tout un environnement humain qu'il convient de coordonner et de faire collaborer. Sans oublier que l'IoT implique souvent une infrastructure Cloud, ce qui ajoute encore à la complexité de cet écosystème.

---

[1] *Common Vulnerability Scoring System* : correspondant à une évaluation standardisée de la criticité d'une vulnérabilité selon des critères objectifs et mesurables, et utilisé par les centres de veille de vulnérabilités tels que le CERT-FR.

[2] *Security Operation Center* : Entité dans l'entreprise chargée de la détection, de la gestion et de la prévention des incidents de sécurité. Il désigne à la fois les moyens humains, l'outillage de collecte et d'analyse de donnée ainsi que l'ensemble des processus correspondants.

1.3 Architecture technique générale

Il faut donc faire collaborer beaucoup d'interlocuteurs, tous issus d'horizons très différents pour assurer un bon fonctionnement et obtenir une bonne protection. Et cela sans même parler de l'hétérogénéité des technologies en jeu dans l'environnement IoT :

D'un point de vue matériel

Le matériel mis en œuvre sur un objet connecté peut être varié et faire appel à des technologies très hétérogènes :

- Capteurs et actionneurs électromécaniques,
- Circuits imprimés dédiés à un usage donné,
- Microprocesseurs, microcontrôleurs ou SoC (System-on-Chip) en fonction des optimisations recherchées et de la versatilité des composants utilisés.

Viennent ensuite potentiellement des problématiques de sécurité, notamment physique, lorsque l'objet est déployé dans l'espace public et qu'on l'on veut assurer la disponibilité du système, son intégrité ou encore la confidentialité des données manipulées.
Assurer la cybersécurité d'un objet connecté nécessite bien souvent de se plonger dans le détail de ses spécifications matérielles ce qui requiert une expertise pointue et relativement rare.

D'un point de vue logiciel

Du côté du logiciel, il faut être conscient du grand écart que l'on doit négocier pour avoir une vue complète de l'écosystème :

- Côté objet, un micrologiciel embarqué est injecté à la fabrication de l'objet. Un micrologiciel qui doit être régulièrement mis à jour. Il est développé dans des langages dits « bas niveau » par des spécialistes et fait le lien entre le monde physique (les capteurs et actionneurs) et le monde IT (la plateforme IoT) ; il s'agit d'un maillon clé dans la cybersécurité de l'ensemble de l'écosystème
- Au centre, dans les mains des utilisateurs, des applications mobiles ou web permettent d'interagir avec les données du système et directement ou indirectement avec l'objet lui-même.
- Côté serveur (ou plateforme IoT), nous retrouvons des applications web, des APIs[3], des logiciels de stockage et traitement de données traditionnellement maitrisés par les entreprises.

D'un point de vue connectivité

- Capteurs et actionneurs peuvent être reliés localement à un objet via des protocoles filaires ou sans fil, plus ou moins propriétaires et plus ou moins répandus : Bluetooth ou BLE (Bluetooth Low Energy), Zigbee, Z-Wave, etc.
- L'objet peut ensuite être connecté à un serveur situé à une grande distance via un réseau sans fil longue-portée (par exemple Sigfox ou LoRaWAN) ou bien via Internet à travers une connexion Wifi ou Ethernet. Cette connectivité peut aussi être assurée par une passerelle à proximité qui peut jouer un rôle de concentrateur d'objets et de relai vers Internet.
- Ces connectivités, locales et longue portée, ont elles-mêmes des caractéristiques propres en matière de niveau de confiance intrinsèque et de cybersécurité.
- La nature des données échangées, le type d'alimentation en énergie de l'objet seront ensuite déterminants concernant le protocole applicatif utilisé : appels d'APIs en HTTP,

[3] *Application Programming Interface* : Interface logicielle permettant l'interaction entre deux applications. Par généralisation, nous traiterons ici des éléments standardisés et prévus pour interagir avec un système IoT (objet et / ou flotte et / ou applicatif centralisé).

envoi/réception de messages sur une file de messages (par exemple : MQTT), etc.

Pour assurer la cybersécurité de bout-en-bout de l'écosystème, il conviendra donc d'en maitriser l'architecture complète (matérielle, logicielle et connectivité) pour pouvoir imaginer les scénarios de risques, identifier des mesures adaptées et réalistes.

1.4 Conséquences sur la cybersécurité de l'objet

C'est donc systématiquement un écosystème entier qu'il faut considérer pour évaluer les risques d'un objet et pouvoir identifier les bonnes mesures de sécurité à mettre en œuvre :

- Un objet connecté interagit avec son environnement physique (par le biais de capteurs et d'actionneurs),
- Il interagit avec des humains en proximité ou le pilotant à distance
- Il interagit également potentiellement avec d'autres objets,
- Il peut communiquer avec une passerelle en proximité,
- Il se connecte et échange des données par le biais de réseau dont le niveau de confiance est variable,
- Enfin il est connecté avec un ou des serveurs situés dans le Cloud (où que celui-ci se trouve).

Cet écosystème est par nature à la fois :

- Distribué dans l'espace, dans des environnements potentiellement non maitrisés,
- Constitué de technologies hétérogènes.

Sa mise en œuvre :

- Nécessite, pour être maitrisée dans son ensemble, différentes compétences et expertises portées par des spécialistes pour qui l'approche cybersécurité traditionnelle n'est pas forcément naturelle et est encore moins un réflexe,
- Connait plusieurs phases qui vont toutes devoir être prises en compte dans l'approche cybersécurité.

Ces caractéristiques, particulières au monde des objets connectés, sont sources de nouveaux risques et ces derniers doivent donc être identifiés et analysés pour être correctement contrés.

1.5 Les risques spécifiques à l'IoT

L'évolution technologique et numérique marque un accroissement exponentiel du nombre d'appareils intelligents interconnectés ayant pour objectif d'apporter plus de confort aux utilisateurs.

Cependant, le confort et les bénéfices de ces appareils, couplés aux failles et vulnérabilités qu'ils présentent ainsi qu'au manque de sensibilisation de leurs usagers par rapport aux menaces qui leur sont liées, représentent plusieurs risques à ne pas négliger.

En effet, les objets connectés ayant déjà commencé à envahir nos écosystèmes (l'étude Gartner[4] de 2017 prédisait déjà 20 milliards d'objets connectés en 2020, ce qui semble s'être concrétisé selon les différentes sources disponibles), les risques en font de même en raison des faiblesses intrinsèques de ces objets.

[4] https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Le nombre d'objets multiplie le nombre de cibles de manière exponentielle. Leur faible niveau de sécurité – celle-ci n'étant parfois pas prise en compte dès la conception – en contrepartie de plus d'agrément ou de fonctionnalités (ports ouverts, services exposés) augmente la surface d'attaque. De plus, le manque d'expertise des utilisateurs des objets – souvent non sensibilisés à la cybersécurité – fait encore baisser la garde d'un cran.

Les risques sont donc nombreux et pour ne citer que quelques exemples :

- Sur la vie privée : les caméras intelligentes, les ampoules intelligentes, les détecteurs d'intrusion, les montres connectées, les jouets intelligents, les véhicules autonomes, les appareils médicaux ou plus généralement tous les objets comprenant des capteurs émettent un grand volume de données de manière autonome. Autant de données sur nos vies privées qui, si elles sont collectées et corrélées, peuvent permettre de reconstituer des informations sensibles (adresses, habitudes, conditions médicales, etc.). Cela peut aller de l'objectif marketing à l'usage criminel.
- Sur la sécurité des entreprises : les systèmes industriels, les capteurs de température et d'humidité en salles serveurs, les badgeuses, etc. communiquent entre eux et la compromission de ce type d'informations – comme le changement d'un paramètre – peut être désastreux, d'autant plus que, vu le maillage et la décentralisation des échanges, il sera de plus en plus difficile de cerner la faille.
- Sur la sécurité des organisations publiques : smart cities – ou villes intelligentes – (gestion du trafic routier, gestion de l'éclairage public, gestion des ordures, gestion de la pollution et de l'environnement, télésurveillance publique, …), hôpitaux… de plus en plus de fonctions sensibles sont déléguées à des appareils intelligents qui, s'ils sont attaqués, auront des impacts humains : sur la sécurité des habitants, voire sur des vies humaines.
- Sur la lutte contre la fraude : fraude à l'assurance ou fraude bancaire, les objets connectés – détournés de leur fonction première – deviennent des atouts intéressants pour déjouer les processus de contrôle mis en place.
- Sur la capacité de rebond : introduction dans le système d'information de l'organisation par le biais d'un objet vulnérable et exploité (par exemple, l'exfiltration des données des joueurs d'un casino à travers un aquarium connecté, ou autres données sensibles).
- Sur la disponibilité même des services connectés, liée à celle d'un fournisseur évoluant dans un marché encore jeune et constitué de nombreux acteurs dont la pérennité n'est pas assurée.

La liste est longue et l'imagination est sans limite pour ces objets dont les capacités sont de plus en plus étendues.

1.6 Les vulnérabilités spécifiques à l'IoT

Les travaux de la fondation OWASP ont mis en avant le top 10 des vulnérabilités les plus fréquemment rencontrées sur les objets connectés[5]

Des mots de passes faibles ou codés en dur

Vulnérabilité liée à l'utilisation d'identifiants facilement piratables par des attaques brute-force, disponibles publiquement ou inchangés (conservation des identifiants par défaut) incluant les backdoors dans les *firmwares* (micrologiciels) ou logiciels clients attribuant des accès non autorisés aux systèmes déployés

Des services réseau non sécurisés

Vulnérabilité liée à l'existence de services réseau non nécessaires actifs sur l'appareil lui-même, spécialement ceux exposés sur internet qui compromettent la confidentialité,

[5] https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

l'intégrité/authenticité ou la disponibilité de l'information, ou permettent une prise de contrôle non autorisée

Des interfaces de l'écosystème non sécurisées

Vulnérabilité liée à la présence d'interfaces Web, API, cloud ou mobiles non sécurisées dans l'écosystème à l'extérieur de l'appareil permettant la compromission de celui-ci ou de ses composants (manque d'authentification/autorisation, manque ou faible chiffrement, manque de filtrage entrant/sortant).

Le manque de mécanisme de mise à jour sécurisé

Vulnérabilité liée au manque de possibilité de mettre à jour l'appareil de façon sécurisée. Cela inclut le manque de validation du *firmware* sur l'appareil, l'absence de chiffrement en transit, de mécanisme anti-rollback (blocage des anciennes versions de *firmware* – application frauduleuse d'anciens paramètres) et le manque de notifications des changements de sécurité dus aux mises à jour.

L'utilisation de composants non sécurisés ou obsolètes

Vulnérabilité liée à l'utilisation de composants/librairies logiciels obsolètes ou non sécurisés pouvant permettre la compromission de l'appareil. Cela inclut une personnalisation non sécurisée des plateformes du système d'exploitation et l'utilisation d'un logiciel ou de composants matériel tiers provenant d'une chaine d'approvisionnement compromise

Une protection de la confidentialité insuffisante

Vulnérabilité issue du stockage non sécurisé d'informations personnelles de l'utilisateur sur l'appareil, ou dans un écosystème qui est utilisé de façon insuffisamment sécurisée / inadaptée ou sans autorisation.

Le stockage ou le transfert de données non sécurisé

Vulnérabilité liée à un manque de chiffrement ou de contrôle d'accès sur les données sensibles à n'importe quel niveau de l'écosystème, incluant au repos, en transit ou pendant le traitement.

Le manque de gestion des appareils en production

Vulnérabilité liée à un manque de gestion des appareils déployés en production, incluant la gestion d'actifs, gestion des mises à jour, décommissionnement sécurisé, monitoring du système et capacités de réaction.

Des paramètres par défaut non sécurisés

Vulnérabilité liée à des appareils ou systèmes déployés avec des paramètres par défaut non sécurisés et manque de possibilité de rendre le système plus sécurisé en restreignant la possibilité des opérateurs à modifier les configurations

Le manque de durcissement physique

Vulnérabilité liée au manque de mesures de durcissement physique, permettant aux attaquants potentiels de prendre le contrôle local de l'appareil ou de récupérer des informations sensibles qui peuvent être utilisées pour de futures attaques

1.7 Cycle de vie de l'objet

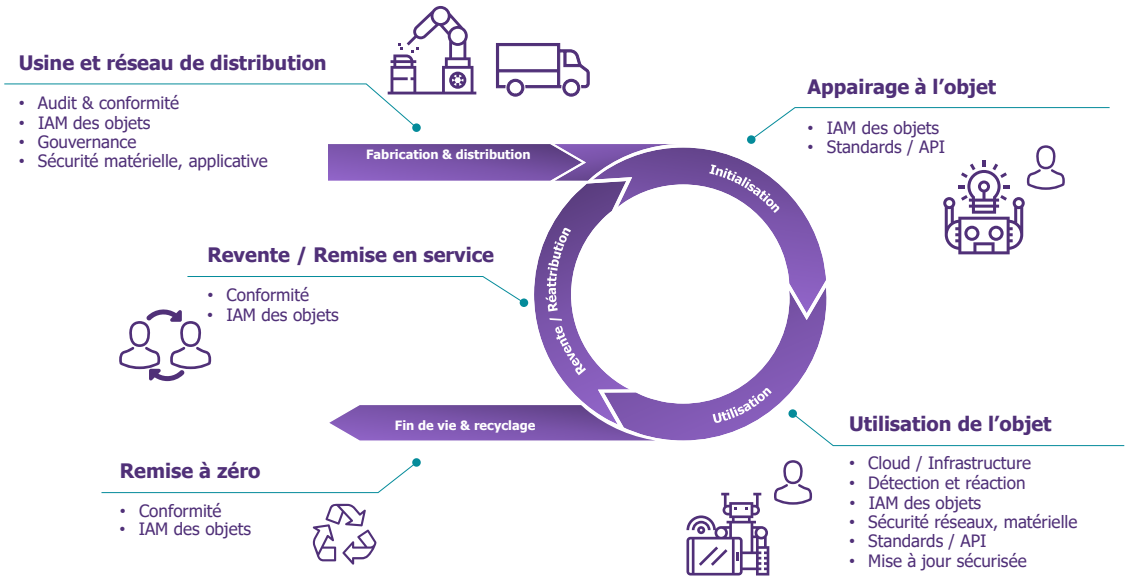
Un aspect essentiel à prendre en compte dans un projet IoT, valable aussi bien pour sa conception fonctionnelle que pour les aspects de cybersécurité dans une approche « security-by-design » est le cycle de vie de l'objet connecté. La prise en compte du fonctionnement de

l'objet à chaque étape ainsi que les différentes interactions qu'il aura avec des utilisateurs ou tout autre composant de l'écosystème doivent également être considérés.

C'est donc lors de la phase de conception qu'il faut anticiper toutes les situations futures, usages nominaux, exceptions, détournements, etc.

À chaque situation, une recherche de scénarios d'attaque ou de vulnérabilités doit être effectuée afin de déterminer les meilleures contremesures, via un matériel plus sécurisé, des contrôles logiciels supplémentaires, un éventuel chiffrement des données au repos ou en transit ou encore un processus adapté et empêchant une faille d'être exploitée.

Enfin à chacune des étapes du cycle de vie d'un objet, présentées dans le schéma ci-dessous, correspondent plusieurs thématiques de sécurisation à mettre en œuvre.



2 Les principaux risques de l'IoT

2.1 Fabrication, distribution, initialisation

2.1.1 Description

Les phases amont du cycle de vie peuvent déjà être la source de nombreux problèmes de sécurité : identifiants initiaux non uniques ou dont la confidentialité n'est pas assurée, obsolescence du logiciel embarqué avant même la distribution et le déballage

2.1.2 Conséquences

- Dès sa fabrication, un secret unique est préférable et le process de fabrication doit garantir sa confidentialité, y compris et surtout s'il fait intervenir des tiers, sous peine de voir une flotte d'objets compromise dans sa globalité.
- La distribution de l'objet doit faire l'objet d'une attention particulière : si ce temps de distribution est long, le logiciel embarqué est peut-être déjà obsolète avant même le déballage ou la livraison de l'objet et sa mise à jour (automatique, voire forcée) est fortement recommandée.
- L'initialisation, si elle ne requiert pas la personnalisation d'un secret par l'utilisateur, peut laisser un accès par défaut à l'objet à un attaquant.

2.1.3 Scénario d'illustration

En 2016, le botnet Miraï[6] est créé à partir de dizaines de milliers de caméras connectées ou routeurs non sécurisés, en exploitant des accès administrateurs par défaut permettant de s'y connecter, d'y injecter une mise à jour qui va elle-même tenter de se connecter à d'autres caméras et se répliquer.

Une fois ce botnet constitué, il sera utilisé dans des attaques DDoS qui restent encore aujourd'hui parmi les plus massives en termes de bande passante utilisée. Des infrastructures critiques pour Internet tels des serveurs DNS seront visées, dégradant l'accès à de nombreux sites Internet populaires et très fréquentés pendant plusieurs heures.

2.1.4 Mesures de sécurité

Lors de ces phases de fabrication, distribution ou d'initialisation des objets connectés, plusieurs mesures de sécurité peuvent être envisagées pour renforcer le niveau de sécurité des objets ensuite déployés :

- Injecter un secret unique suffisamment robuste par objet (cf. Recommandation R19 de l'ANSSI dans son Guide de Sécurité des Systèmes d'Objets connectés[7]).
- Éviter les secrets partagés (et préférer l'utilisation de cryptographie asymétrique avec une attention particulière sur la sécurité de la clé privée, et si le contexte le permet un stockage sécurisé physiquement de cette dernière).
- Définir avec attention le process de fabrication et les tiers intervenants pour minimiser les risques de fuites.
- Forcer une personnalisation des identifiants de connexion lors de la première utilisation
- Faire en sorte qu'un objet non initialisé ne puisse exposer ou contacter que des APIs permettant uniquement son initialisation.

---

[6] https://fr.wikipedia.org/wiki/Mirai_(logiciel_malveillant)

[7] https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-securite_des_systemes_objets_connectes_iot-v1.0.pdf

2.2 Attaques par rebond

2.2.1 Description

Le risque d'attaque par rebond est très présent au sein des entreprises. En effet, ce type d'attaque pluridisciplinaire cherche à exploiter la moindre faille du SI pour s'y introduire et compromettre un maximum de systèmes. Les vulnérabilités techniques, organisationnelles, physiques ou encore humaines rendent la surface d'exposition importante et d'autant plus complexe la détection ou réponse à ces attaques.

Ces attaques sont furtives et cherchent à impacter un maximum de systèmes. La première étape pour les attaquants consiste à trouver ou créer une porte d'entrée dans le SI. Dans un second temps, l'attaquant se déplace au sein du réseau en trompant les systèmes de défense en place pour obtenir des privilèges élevés et ouvrir les portes jusqu'à son objectif.

Les objets connectés démultiplient ce risque d'attaque par rebond en offrant une surface d'attaque plus large.

2.2.2 Conséquences

La compromission d'un objet permettant l'accès à son SI et aux actifs même non vulnérables peut entrainer des conséquences multiples, par exemple :

- Un chiffrement par rançongiciel, empêchant les utilisateurs et l'entreprise d'accéder à leurs données et d'utiliser leurs applications.
- Un vol de données **critiques** comme les savoir-faire de l'entreprise, une base de données relative aux clients, ou encore des données financières
- Une atteinte à l'intégrité des systèmes industriels ; dans certains cas l'attaque vise à endommager les systèmes de production de l'entreprise et pénètre jusqu'aux automates de production

2.2.3 Scénario d'illustration

En 2018[8][9], un hacker s'est introduit dans la base de données d'un casino en se servant d'un thermomètre connecté au réseau de l'établissement dans l'aquarium du hall d'entrée. C'est un des cas les plus connus en matière de compromission IoT suivie d'un rebond au sein du SI de l'entreprise.

Le **pirate** a pu exfiltrer une quantité importante de données envoyées par ce biais sur un appareil en Finlande, soit 10 Go d'informations confidentielles telles que les bases de données des « high roll », c'est-à-dire des joueurs qui misent d'importantes sommes d'argent.

Le système d'information du casino a ainsi été piraté *via* un thermomètre, permettant au pirate de prendre le contrôle des caméras, des portes de sécurité, jusqu'à arriver aux données personnelles des joueurs et des employés.

2.2.4 Mesures de sécurité

Cloisonnement des réseaux

L'utilisation de pares-feux et DMZ permettent de séparer les services, les actifs critiques, ou les catégories d'équipements par domaines de responsabilité, afin de limiter leur

[8] https://iotsecuritywatch.com/2018/06/21/un-casino-pirate-a-cause-dun-thermometre-connecte-dun-aquarium/

[9] https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

compromission en cas d'intrusion et dans ce cas précis les capacités de rebonds et le nombre de machines compromises.

Durcissement des systèmes

L'application de règles de base « d'hygiène » permet de réduire considérablement le risque de compromission. Parmi ces mesures :

- Le changement des mots de passe par défaut,
- Leur complexification et leur renouvèlement périodique (i.e. rotation des clés),
- La revue des paramétrages « par défaut » et l'activation d'un maximum de fonctionnalités de sécurité de l'appareil,
- La suppression des services non nécessaires,
- La restriction des accès utilisateur et administrateur etc…

Maintien en conditions de sécurité

Une vulnérabilité présente sur l'objet connecté correspond au premier maillon d'une attaque par rebond. Il convient alors d'anticiper ces vulnérabilités et de les corriger tout au long de la vie de l'objet. Cela peut être fait au travers des processus de suivi, correction et déploiement de correctifs au niveau des systèmes, des applications ou encore des protocoles réseau.

2.3 Accès non autorisé aux API

2.3.1 Description

Tous les composants de l'écosystème sont susceptibles d'exposer des APIs, un accès non sécurisé ou non autorisé à ces dernières est la source de ce risque ; les risques sont multiples selon l'angle d'approche :

- Dans une approche locale, c'est l'objet qui est visé : il faut considérer les cas où l'objet est équipé d'un port de connexion local avec ou sans fil. Il pourrait en résulter un excès de confiance si l'on considère que la nécessité de proximité est une mesure de sécurité suffisante.
- Dans une approche distante, aussi bien un objet unitaire que la flotte entière ou le système centralisé peuvent être visés. En effet, la compromission d'une API centrale consommée par un objet peut entrainer un défaut d'intégrité ou de confidentialité des données de l'ensemble du système. L'étendue de la compromission peut dans ce cas être très importante.

2.3.2 Conséquences

Les conséquences de ce type de risque vont être liées au potentiel de l'API exploitée.

Avec la compromission d'une **API de consultation**, la conséquence première est la récupération indue d'informations, avec le risque légal qui en découle. Une perte de données est également possible dans le cas où la collecte est considérée du point de vue de l'objet comme un acquittement lui permettant de recycler la mémoire dont le contenu vient d'être récupéré. Cette compromission peut également permettre une part d'espionnage industriel, notamment si l'API permet la collecte de données métier.

Les **API de collecte d'information** vers le référentiel central peuvent également être altérées par l'injection de données erronées visant à intoxiquer celui-ci.

Les compromissions des **API de contrôle** d'un objet sont les plus spectaculaires et sont donc celles qui ont le plus fort impact de notoriété. Selon l'avancée de la compromission et le potentiel de l'API, il devient parfois possible de détourner l'objet de son but premier.

Enfin, une **API de configuration de la flotte d'objets** permet l'enregistrement et la sécurisation des objets dans la flotte. Sa compromission peut avoir des conséquences supplémentaires car il devient possible de recenser l'intégralité de la flotte en disposant d'un

accès « de confiance » avec chaque objet, même à distance. Contrairement aux points précédents, cette compromission touche plusieurs objets et peut aller jusqu'à compromettre la totalité du parc.

2.3.3 Scénario d'illustration

La compromission d'API peut être illustrée par l'*exploit* réalisé par Charlie Miller et Chris Valasek, présenté à la conférence *Black Hat* de 2015 (https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ ; Le *white paper* est également disponible : Remote Car Hacking.pdf (illmatics.com))

En décodant le mode de génération des mots de passe Wi-Fi, les attaquants ont pu accéder à l'unité de contrôle multimédia, puis rebondir vers l'unité centrale.

À partir de l'unité centrale, ils ont exploité des faiblesses triviales des composants pour accéder aux API du système de guidage et du système multimédia.

Cette compromission leur a non seulement permis de tracer, à l'aide du GPS du véhicule, le trajet de celui-ci mais également d'activer certaines commandes à distance (climatisation, diffusion sonore…). Une version plus avancée de leur exploitation de faille a même permis le contrôle de la direction et de la transmission du véhicule.

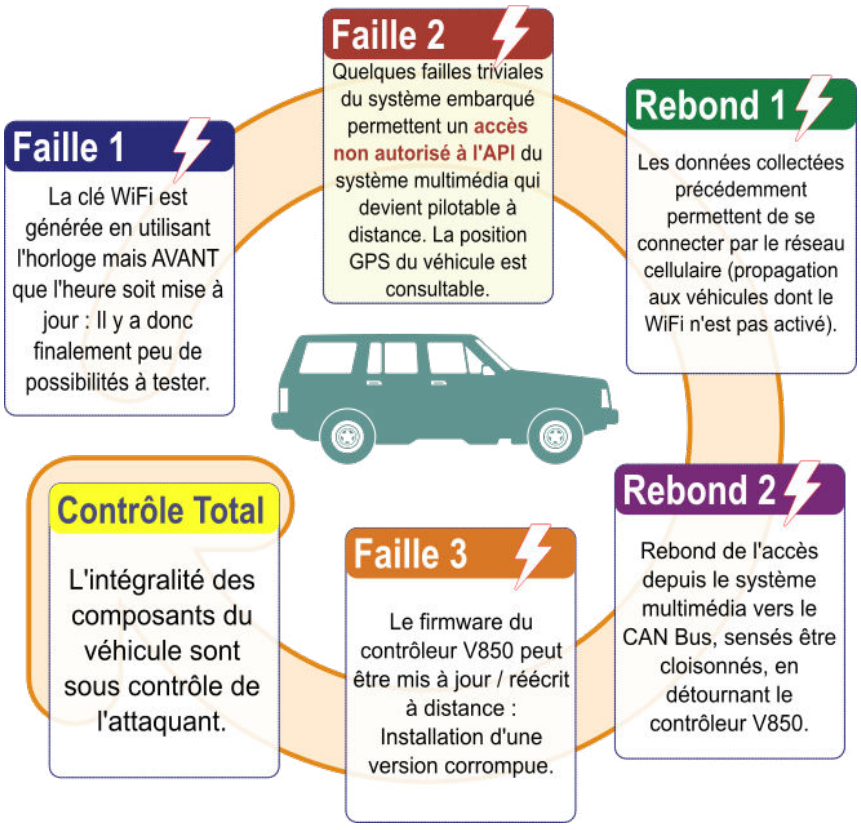


Figure 1 : Étapes de la compromission d'une Jeep Cherokee

2.3.4 Mesures de sécurité

Chiffrement et authentification

Tout accès à une API requiert un chiffrement / une authentification. Les protocoles en clair ne doivent pas être utilisés.

Principe du moindre privilège

Chaque utilisateur / compte doit disposer des privilèges les plus faibles possibles.

Réduction des points d'entrée

Les points d'accès (physiques et logiciels) doivent être masqués. L'API doit regrouper uniquement les fonctions nécessaires et suffisantes pour l'emploi attendu : principe du plus faible potentiel. Cette mesure est détaillée au paragraphe « 3.6 Minimisation de la surface d'attaque ».

2.4 Fuite de données

2.4.1 Description

Le risque principal sera de type **divulgation** : des données confidentielles (personnelles ou industrielles) sont accessibles à des tiers non autorisés.

Le risque secondaire sera de type **rebond** : les données permettent de faciliter d'autres manipulations malveillantes.

L'accès illicite aux données peut être réalisé selon les contextes directement sur l'objet, la flotte, les serveurs ou les canaux de transmission. Il couvre donc l'intégralité des éléments du système.

2.4.2 Conséquences

- Liées à l'espionnage industriel : les données récupérées peuvent fournir des informations sur la conception des produits, des informations internes…
- Légales : notamment par la divulgation de données personnelles encadrées par le RGPD[10]
- Appuis à l'ingénierie sociale : il peut y avoir suffisamment d'informations ou d'éléments considérés comme internes et réutilisables pour biaiser une relation de confiance.
- Faille logicielle : ces données peuvent constituer un point de départ pour une identification auprès d'autres sous-systèmes, un rebond…

2.4.3 Scénario d'illustration

Les cas avérés et rendus publics autour de ce risque sont les plus répandus, notamment au travers des caméras connectées. La récente publication d'une possibilité de récupération des images des caméras de la société Verkada en est un bon exemple (https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams).

Dans ce scénario, les assaillants sont parvenus à s'authentifier en tant que super administrateur des caméras, leur procurant la possibilité de consulter les flux vidéo et audio en direct des caméras, ainsi que les vidéos stockées sur celles-ci. Les caméras étant déployées comme réseaux de surveillance d'entreprises et d'établissements publics, les informations collectées touchent à la fois au secret industriel et aux informations personnelles.

Par extension, sans contourner des mesures de contrôle d'accès, il existe parfois un risque lié à une diffusion incontrôlée ou aux conséquences d'une diffusion trop ouverte des données. En 2018, Nathan Ruser illustrait avec les « heatmaps » issues de Strava — un traceur GPS couplé à des fonctionnalités de réseau social, utilisé par les sportifs — les positions de « centres de vie », permettant par exemple de localiser des bases militaires : https://www.nytimes.com/2018/01/30/world/australia/strava-heat-map-student.html et https://twitter.com/Nrg8000/status/957318498102865920.

[10] *Règlement Général sur la Protection des Données* : https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

2.4.4 Mesures de sécurité

Hormis les mesures « classiques » permettant de préserver les accès aux serveurs, aux flux de communication et à la flotte, les spécificités de l'IoT doivent être prises en considération :

- Les objets devraient disposer et manipuler le minimum de données nécessaires à leur action. Il s'agit de points de fuites de prédilection par leur éloignement physique. L'anonymisation est également une bonne pratique à favoriser pour limiter l'exploitation des données collectées. Un audit des données exploitées par chaque objet permet de jauger le risque d'un accès non autorisé.
- Le chiffrement des données manipulées peut également constituer un rempart pour préserver leur confidentialité en cas de fuite. Cette mesure est efficace si les secrets permettant ce chiffrement ne sont pas également vulnérables.
- Les interfaces locales et serveur distant doivent être considérées comme accessibles publiquement et sécurisées en conséquence : authentification multi-facteur, segmentation réseau, désactivation des interfaces non utilisées, etc.
- La multitude des objets en action implique que la sécurisation de chacun doit être unique : un mot de passe permettant un accès local doit être personnalisé, et un secret permettant de se connecter à l'infrastructure ne doit pas être le même pour tous les objets…
- Les réseaux utilisés, s'ils ne les gèrent pas nativement, peuvent nécessiter l'implémentation de mécanismes de sécurité (authentification serveur et/ou mutuelle, chiffrement) en fonction de la sensibilité des données. Il faut alors envisager de prendre des mesures complémentaires au niveau applicatif.

Spécificités du fournisseur ou fabricant d'objets connectés

Dans le cas d'objets connectés achetés auprès d'un fournisseur, des pratiques de sécurisation supplémentaires sont nécessaires.

Du point de vue du *fournisseur* d'objets connectés :

- Tout mécanisme de type backdoor (porte dérobée) est à proscrire. Dans le cas où ce type de mécanisme a été mis en œuvre durant la mise au point de l'objet, il doit être retiré —et non simplement désactivé— sur les objets commercialisés.
- La sécurisation des accès doit être prévue « par défaut » : soit avec un mot de passe par défaut différent pour chaque objet, soit avec l'obligation de modification / définition d'une identification à l'inclusion de l'objet dans la flotte.
- Toutes les interfaces (physiques et logiques) doivent être documentées pour cartographier exhaustivement les risques.

Du point de vue du *consommateur* d'objets connectés :

- Réaliser l'inventaire des interfaces (physiques et logiques) et s'assurer de leur sécurisation, même celles qui ne sont pas employées.
- Le fournisseur de l'objet peut avoir un accès à celui-ci, qui peut être mis en place pour des besoins de maintenance… Cet accès doit être au moins documenté ou mentionné, et, idéalement, encadré —contrat, conditions générales d'utilisation, plan d'assurance sécurité…

2.5 Revente, réattribution, fin de vie, obsolescence

2.5.1 Description

Ces risques surviennent lorsque la fin du cycle de vie de l'objet n'a pas été correctement anticipée et qu'un processus de gestion de l'objet est détourné de son déroulement nominal.

2.5.2 Conséquences

Ce risque peut entrainer une fuite de données locales ou distantes, faciliter la réutilisation après un vol de l'objet ou encore un détournement du fonctionnement nominal de l'objet.

Le recyclage ou la revente peuvent facilement être ignorées lors de la conception de l'objet et cela peut entrainer des conséquences avec de forts impacts :

- Prise de contrôle de l'objet par son ancien propriétaire
- Divulgation des données de l'ancien utilisateur au nouveau propriétaire
- Non-dissuasion du vol d'un objet

2.5.3 Scénario d'illustration

De nombreux chercheurs en sécurité ont pu mettre en évidence des oublis de définition de processus de fin de vie pour les objets connectés et ont pu par exemple, en accédant à des ampoules connectées jetées en fin de vie, démontrer que des informations sensibles, des mots de passe Wi-Fi par exemple, persistaient dans leurs espaces de stockage même une fois l'ampoule inopérante[11].

2.5.4 Mesures de sécurité

Afin d'anticiper la réutilisation, revente ou fin de vie de l'objet, il convient de réaliser un inventaire le plus complet possible des données manipulées, qu'elles soient stockées localement sur l'objet ou bien dans l'infrastructure cloud.

Une fois cet inventaire réalisé, il est fortement recommandé de permettre à l'utilisateur de supprimer ces données – tel que prévu à l'article 17 du RGPD – (non sans lui laisser l'option de les exporter pour son usage propre) afin qu'elles ne soient pas divulguées à un tiers (futur utilisateur ou propriétaire, chercheur un peu curieux, etc.)

Dans un contexte d'entreprise, un inventaire des objets avec leur statut et les utilisateurs finaux associés est également un outil important à mettre à disposition d'un gestionnaire de flotte, ainsi que des fonctionnalités de réinitialisation à distance en cas de vol/perte ou suspicion de compromission d'un objet.

Il convient aussi de formaliser une procédure de mise au rebut/réattribution/réinitialisation pour l'utilisateur final (ou le gestionnaire d'une flotte) permettant l'effacement des données voire la destruction contrôlée des objets.

Une question mérite d'être abordée lors de la conception de l'objet sur les mécanismes permettant une revente :

- L'ancien propriétaire doit-il explicitement se dés-appairer de l'objet avant de permettre à un nouveau de s'en servir (cas d'un smartphone associé à un compte utilisateur du fabricant) au risque de rendre l'objet inutilisable par son nouveau propriétaire si ce dés-appairage n'est pas réalisé ?
- Ou bien un nouvel utilisateur a-t-il la possibilité de réinitialiser un objet sans le concours du précédent ? Au risque de faciliter voire inciter le vol de tels objets.

Enfin, il reste la problématique de l'obsolescence d'un objet du maintien de l'infrastructure à laquelle il est connecté. Une fois la commercialisation arrêtée :

- Combien de temps le fournisseur va-t-il permettre l'utilisation des objets vendus ?
- Combien de temps des mises à jour, correctifs fonctionnels ou sécurité continueront-ils à être distribués ?

En cas de décommissionnement ou d'indisponibilité de l'infrastructure (par exemple en cas de disparition du fournisseur) l'objet pourra-t-il être utilisé sans ses fonctionnalités connectées ?

---

[11] https://www.zdnet.fr/actualites/comment-cette-ampoule-intelligente-divulguait-votre-mot-de-passe-wi-fi-entre-autre-39880163.htm

Sera-t-il acceptable d'utiliser un objet potentiellement vulnérable car plus mis à jour ? Par ailleurs, comment l'objet doit-il fonctionner dans ce cas dégradé ? Par exemple : une serrure intelligente déconnectée doit-elle rester verrouillée ou se déverrouiller par défaut ?

3 Principes de sécurisation

Les IoT font partie d'un environnement complexe et leur sécurisation seule ne saurait prévenir les risques d'attaque sur un SI. Au regard de la diversité et de la complexité des risques liés aux attaques, des mesures doivent être prises à l'échelle de l'entreprise et de son SI.

Il faut adopter une stratégie de défense en profondeur pour compartimenter les éléments composant le SI et mettre en place différentes approches de sécurisation :

Sensibilisation des collaborateurs à la SSI

La formation des collaborateurs est une des clés pour la sécurité d'un SI car ils représentent un risque considérable en raison des menaces utilisant l'ingénierie sociale (emails malveillants, supports amovibles infectés) ou simplement l'exploitation d'erreurs humaines.

Conformité avec un standard de sécurité

Il existe un certain nombre de standards, guides ou méthodologies de sécurité des systèmes d'information tels que ISO 2700X, ENISA, NIST, etc… Ces documents visent à aider les entreprises à structurer leur défense en listant des points de contrôle transverses pour le SI, c'est-à-dire sur les plans techniques, organisationnels ou même de sécurité physique des systèmes d'information.

Mise en place de solutions de sécurité éprouvées

Certaines agences telles que l'ANSSI éprouvent et certifient différentes solutions de sécurité disponibles sur le marché et publient des conseils sur la mise en œuvre de mesures de sécurité en fonction des besoins de l'entreprise.

Plan de gestion de crise et reprise d'activité

La capacité de détection et réponse aux incidents d'une entreprise est un facteur crucial pour limiter l'impact d'une attaque et si elle fait défaut, une attaque mineure peut se transformer en crise majeure et aller jusqu'à mettre en péril la pérennité de l'entreprise.

Un plan de réponse à incident doit donc être formalisé et régulièrement testé pour en garantir l'efficacité et l'applicabilité.

Les principes généraux de sécurité cités ci-dessus, même s'ils ne sont pas exhaustifs, contribuent à renforcer le niveau de sécurité informatique du SI et par extension des objets qui y sont connectés.

En complément des mesures de sécurité doivent également être prises au niveau des IoT afin qu'ils ne mettent pas en péril le SI à leur tour.

3.1 Analyse de risques spécifique IoT

Assurer la cybersécurité d'un écosystème connecté peut (et doit) passer par une méthodologie classique, habituelle et éprouvée d'analyse de risques permettant l'identification et la priorisation de ces derniers. Cette analyse faite, la définition des mesures face aux risques et leur mise en œuvre doivent être pilotées.

Il est toutefois nécessaire de garder en tête que, si la méthodologie est similaire, elle doit, pour être pleinement efficace, s'adapter aux spécificités de l'écosystème IoT, vecteur de nouveaux risques et de nouveaux scénarios de vulnérabilités :

- Le lien avec le monde physique via des capteurs et actionneurs ou encore le nombre important d'objets déployés et la nature potentiellement non maitrisée de leur environnement (accès public, lieux plus ou moins fréquentés et surveillés, objet sous le contrôle légitime d'un tiers ou d'un client, etc.).
- L'hétérogénéité et parfois l'exotisme des technologies employées nécessitant de coordonner un nombre important de personnes et de compétences.
- La sensibilité et le volume des données manipulées et échangées.
- Les limitations matérielles (puissance de calcul, alimentation électrique, stockage, etc.) et les contraintes que cela impose au moment de la conception, de l'usage et des mises à jour.

De même, au-delà de ces nouveaux risques et de ces nouvelles menaces, il convient d'avoir en tête certains principes et certaines mesures de sécurité complémentaires, propres au domaine des objets connectés :

- Un accès physique à l'ensemble d'une flotte est difficile pour un attaquant. Et si le scénario de compromission d'un objet doit être sérieusement pris en compte, il conviendra de travailler à empêcher un rebond sur le reste de la flotte.
- L'hétérogénéité des technologies utilisées est également une opportunité de travailler à une architecture maitrisée, définissant des points d'interface précis entre les composants pour en assurer la sécurité.
- Très souvent, les données manipulées par un écosystème IoT représentent une valeur immédiate et long terme pour le métier mais il est fréquent que seules des données récentes représentent un intérêt pour un attaquant.
- Enfin, les capacités limitées d'un objet permettent de réduire à un petit nombre les fonctionnalités à sécuriser et les scénarios d'attaque à éprouver.

C'est ainsi que la base de connaissances sur laquelle s'appuie l'analyse de risques doit être enrichie de risques redoutés et de mesures de sécurité propres au monde IoT, ce qui la rendra plus pertinente et complète et donc bien plus utile pour identifier les bons points d'attention et les bonnes mesures de sécurité.

3.2 Minimisation de la surface d'attaque

Une fois l'analyse de risque menée, un point clé à garder en tête lors de la conception d'un objet, lors de son évaluation sécurité ou encore lors de son intégration à un système d'information plus large est le principe de minimisation de la surface d'attaque. En effet, moins l'objet et son écosystème exposent d'éléments, de fonctions et de données collectées susceptibles d'être abusés ou détournés, plus le risque d'exploitation d'une vulnérabilité est réduit.

Un exemple parlant est l'ouverture des ports réseau : certains pourraient être ouverts vers l'extérieur alors qu'une écoute sur la boucle réseau locale (i.e. *localhost*) est tout à fait suffisante. Parfois certains protocoles sont exposés par un logiciel présent par défaut sur le système embarqué sans réel besoin (port d'administration SSH, port HTTP, etc.).

Ce sont autant de portes auxquelles un attaquant peut frapper en espérant trouver un serveur

s'exécutant dans une version ancienne et vulnérable, requérant un mot de passe trop simple ou laissé par défaut.

De plus, en étudiant plus finement les cas d'usages qui, en théorie, requièrent une ouverture de port (recevoir une commande, répondre à un signal de vie, etc.), nous trouvons souvent une approche alternative, généralement plus sécurisée et bien souvent plus efficace du point de vue de l'architecture. Par exemple, un objet qui doit recevoir une commande peut tout à fait initier la connexion, soit périodiquement, soit la maintenir active, et recevoir à travers cette connexion toute commande nécessaire plutôt que de laisser un port ouvert.

Mais la minimisation de la surface d'attaque peut s'appliquer à tous les niveaux de l'écosystème. Certaines mesures ne doivent pas être négligées :

- Une API permettant plus d'actions que celles strictement requises par les cas d'usages fonctionnels
- Un accès non restreint à la console du système embarqué
- L'exécution de modules avec un utilisateur privilégié (i.e. root)
- Le stockage (sur l'objet lui-même ou bien côté serveur) ou l'échange non indispensable de données sensibles
- Le manque de cloisonnement réseau
- Le manque de durcissement physique de l'objet et de ses composants (scellement d'un boitier, résinage des cartes électroniques, etc.)
- La non-détection d'ouverture du boitier de l'objet (ne pas oublier que les objets connectés sont souvent déployés dans un milieu non contrôlé, voire hostile et la menace d'une rétro-ingénierie « sauvage » est bien présente)
- La non-détection d'anomalie de fonctionnement et la mise en sécurité
- Une verbosité des journaux trop importante

Attention toutefois à ne pas imaginer que ce principe de minimisation vise à obtenir une « sécurité par l'obscurité » et il ne faut pas tomber dans cette approche qui peut apporter un faux sentiment de sécurité. Il s'agit bien de limiter les capacités et ressources de l'objet et son écosystème au strict minimum pour remplir sa fonction à un moment donné.

3.3 Configuration des objets

La configuration des objets est un sujet qui présente deux facettes :

- D'une part, le fournisseur d'objet doit prévoir des possibilités de paramétrage permettant à l'objet de réaliser ce pour quoi il est conçu, tout en offrant un niveau de sécurité suffisant.
- D'autre part, le consommateur de l'objet doit être en mesure de paramétrer celui-ci et d'en assurer la sécurisation.

Un aspect transverse à ces deux facettes est que la configuration de l'objet *devrait* inciter le consommateur à sécuriser son objet.

La démarche à adopter par le fournisseur est donc d'adopter une configuration sécurisée par défaut. Ainsi, sans action supplémentaire, la situation est déjà favorable. De plus, l'incitation à la sécurisation est initiée : *Je dispose d'un objet dont l'initialisation me place déjà dans une posture défensive.*

Par ailleurs, la législation évolue rapidement et certains pays envisagent d'interdire par exemple l'utilisation de mots de passe par défaut[12].

Cette démarche ne doit cependant pas être empruntée au détriment de la simplicité pour le

[12] https://www.clubic.com/antivirus-securite-informatique/actualite-396687-peut-on-interdire-les-mots-de-passe-par-defaut-c-est-ce-que-veut-le-gouvernement-britannique.html

https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

consommateur, au risque de perdre son adhésion et le bénéfice sécuritaire ou d'usage général. La mise à disposition de procédures simples, l'accompagnement dans l'initialisation et le maintien en conditions opérationnelles tenant systématiquement compte des risques sont indispensables.

Enfin, si l'on laisse la possibilité à l'utilisateur de désactiver des mécanismes de sécurité activés par défaut, il faut rendre la manipulation suffisamment explicite pour que l'utilisateur soit conscient des conséquences possibles sur la sécurité de l'objet.

3.4 Mesures fournisseurs & opérateurs

Afin d'assurer un niveau de sécurité satisfaisant des objets connectés, cette problématique doit être prise en compte dès la conception du produit et tout au long de son cycle de vie.

Même si aujourd'hui la règlementation est peu développée et n'impose que peu de mesures de sécurité, il appartient à chacun de s'assurer de la mise en œuvre d'un minimum de bonnes pratiques. Bonnes pratiques que l'on peut facilement retrouver dans des guides et standards faisant référence (ANSSI, ENISA, NIST, ETSI, etc.)

À la conception, la responsabilité est donc partagée entre :

- Le fabricant du matériel IoT qui se doit de :
    - Concevoir le matériel selon les exigences minimales de sécurité
    - Protéger l'appareil contre les intrusions et les falsifications
    - Intégrer la sécurité au matériel si le cout le permet
    - Fiabiliser et sécuriser les mises à jour
- Le développeur de la solution logicielle de l'IoT qui se doit de :
    - Respecter une méthodologie ou un framework de développement de logiciels sécurisés : dès la conception, inclure la sécurité dans les outils et les processus
    - Intégrer des API, des bibliothèques et/ou des logiciels open source avec précaution
    - Ne pas négliger les phases de tests de sécurité aux différentes étapes de développement
    - Prévoir les mécanismes permettant une mise à jour sécurisée (i.e. assurant un contrôle d'intégrité) des objets tout au long de leur cycle de vie. Des recommandations sur les bonnes pratiques d'implémentation de ce mécanisme sont par exemple disponibles dans le guide ANSSI PA-087.
- Il peut par exemple avoir recours à des simulateurs et jumeaux numériques pour anticiper les différents scénarios d'attaque et prévoir les contremesures les plus adaptées.

Puis, tout au long du cycle de vie de l'objet, d'autres acteurs entrent en scène :

- L'intégrateur ou responsable de déploiement de l'appareil qui se doit de :
    - Choisir des partenaires éprouvés et s'assurer d'avoir des engagements contractuels incluant des mises à jour régulières du logiciel.
    - Respecter le mode de déploiement prévu par le fabricant et ne pas apporter de modifications
    - Porter une attention particulière à la sécurisation des clés d'authentification (utilisation et stockage)
- L'opérateur ou responsable de l'exploitation de l'appareil qui se doit de :
    - Protéger physiquement l'infrastructure IoT
    - Protéger le système contre les activités malveillantes
    - Réaliser une supervision de l'appareil et son écosystème
    - Effectuer des audits de sécurité réguliers
    - Garder le système à jour
    - Sensibiliser les usagers

Ainsi, lors de la sélection de l'objet et sa mise en production, l'entité utilisatrice devra évaluer

chacune des parties prenantes pour garantir la bonne application des principes de sécurité énoncés ci-dessus.

3.5 Gestion des vulnérabilités

La mise en place d'un processus de gestion des vulnérabilités est un incontournable. Ce processus doit comprendre :

- Le canal de *Vulnerability Disclosure* clairement identifié,
- La veille sécurité sur les composants de l'objet,
- La méthodologie de classification des vulnérabilités (sévérité, urgence, statut),
- Les moyens techniques et organisationnels de correction,
- Le suivi de la réponse donnée.

Les objets connectés étant par nature dispersés, et potentiellement diffusés auprès du grand public, détecter et remédier aux vulnérabilités doivent être prévus dans ce contexte. La diffusion implique la mise en place de canaux d'information bidirectionnels :

- La mise à disposition de correctifs doit pouvoir être indiquée rapidement aux personnes concernées, que ce soient les gestionnaires de flottes internes ou externes ou le grand public,
- Et la remontée de problèmes identifiés par les utilisateurs ou la veille de sécurité doit pouvoir être réalisée aisément, sous peine de perdre une partie de ces remontées.

Un autre aspect de la détection, concernant à la fois les fournisseurs et les exploitants d'objets connectés, repose sur la veille et la prévention. L'identification des vulnérabilités connues[13] qui impactent le catalogue d'objets ou les composants fournit les pistes pour une prise en compte rapide.

D'autres outils comme le *Bug Bounty* ou le *Honey Pot* — objets volontairement exposés sur le réseau et surveillés pour identifier des attaques, réussies ou non, en particulier par des scanners automatiques — améliorent la qualité de la veille.

Les correctifs de ces vulnérabilités doivent être diffusés à la flotte d'objets. Idéalement, ces mises de sécurité empruntent le même canal que les mises à jour fonctionnelles avec une fréquence plus importante.

3.6 Capacité de mise à jour incluses dans les objets

Afin d'assurer la sécurité logicielle des objets IoT, et au-delà des considérations initiales de minimisation de la surface d'attaque (restriction du système aux seules applications, exécutables et pilotes nécessaires au bon fonctionnement du dispositif ; vérification du logiciel aux différentes étapes du démarrage), il sera nécessaire de prévoir les mécanismes de mises à jour logicielles des objets tout au long de leur cycle de vie et pour toute la durée supportée.

Mises à jour logicielles

Les mécanismes de mises à jour logicielles doivent inclure :

- La possibilité de réaliser des mises à jour de micrologiciels et des logiciels embarqués dans l'objet, afin de permettre la correction des erreurs et la distribution de correctifs pour les vulnérabilités qui seront identifiées lors de la vie de l'objet. Ces mises à jour devront disposer d'un numéro de version, et être authentifiées (authentification du logiciel et de sa version au moins, contrôle d'intégrité fortement recommandé)
- La présence par défaut d'un mécanisme antiretour arrière (anti-rollback), interdisant l'installation d'une version de logiciel plus ancienne que celle installée afin d'éviter

[13] https://www.researchgate.net/publication/342588114_CVE_based_classification_of_vulnerable_IoT_systems

l'exploitation de vulnérabilités connues et déjà corrigées ; le contournement de ce mécanisme doit être évité autant que possible, et contrôlé par un mécanisme d'administration sécurisé, s'il doit être implémenté

- Une vérification de l'authenticité et de l'intégrité des mises à jour, par rapport à un acteur de confiance, doit être prévue, idéalement par l'objet lui-même, ou par un autre dispositif intermédiaire en proximité de l'objet (par exemple par la vérification d'une signature électronique du logiciel par son fabricant).
- Un mécanisme de récupération automatique doit également être implémenté, afin de permettre le retour à la dernière bonne configuration connue du logiciel de l'objet dans le cas où un process de mise à jour viendrait à mal se dérouler (par exemple : interruption du process de mise à jour, mauvaise intégrité du pack logiciel)

Réseau de communication

- La transmission de ces mises à jour doit être effectuée au travers de canaux de communication sécurisés, et ininterrompus afin de protéger les objets d'attaques de type phishing. Les protocoles de communication employés devront permettre d'assurer l'authentification de l'origine d'une connexion, ainsi que la confidentialité et l'intégrité des échanges (protocoles standardisés tels que IPsec ou TLS)

  Afin de réduire la surface d'attaque des dispositifs et de limiter les possibilités de cartographie de systèmes connectés à internet, les requêtes dont l'origine n'est pas maitrisée ne devraient pas être traitées (en contrôlant par exemple l'origine des connexions au dispositif par une authentification cryptographique ou par l'organisation du réseau dans lequel ils s'inscrivent).

Gestion du parc IoT

Afin de maitriser la sécurité du parc IoT, une gestion de ce parc doit être mise en place, permettant de remonter le statut de mise à jour de chacun des objets.

Par ailleurs, une veille sur la gestion du cycle de vie des IoT par leur fabricant devra être instaurée, afin de pouvoir identifier les fins de maintenance sur ceux-ci devant conduire au remplacement des objets concernés.

Mises à jour matérielles

Enfin, dans certains cas extrêmes, un rappel de composant peut être nécessaire, lorsque par exemple l'objet concerné ne peut pas faire l'objet d'une mise à jour en l'état, et nécessite de réaliser un remplacement de matériel sur celui-ci (voire de l'objet lui-même) pour atteindre un niveau de sécurité satisfaisant.

4 Conclusion

Au-delà de ce document qui se veut être une introduction aux risques principaux et mesures de sécurité à envisager et vérifier lors de la conception ou l'acquisition d'objets connectés, un certain nombre de guides publiés par des organismes indépendants permettront d'approfondir le sujet :

- **ANSSI** : Recommandations Relatives À La Sécurité Des (Systèmes D') Objets Connectés[14]
- **ENISA** : Guidelines for Securing the Internet of Things[15]
- **NIST** : IoT Device Cybersecurity Capability Core Baseline[16]
- The OWASP Internet of Things Project[17]

Au-delà du respect de bonnes pratiques, selon Guillaume Poupard, directeur de l'ANSSI, *« La sécurité de l'Internet des objets constitue aujourd'hui, et de plus en plus, un important challenge pour la sécurité des données personnelles.*

Un processus de labellisation doit être mis en place sur tous les objets connectés, spécialement dans le domaine industriel. »

Il a également ajouté que l'évaluation des objets connectés grand public et plus low-cost serait plus couteuse et longue. Ainsi, des évaluations plus légères ou des autoévaluations représenteraient des solutions viables pour une meilleure sécurité.

[14] https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-securite_des_systemes_objets_connectes_iot-v1.0.pdf

[15] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport

[16] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf

[17] https://owasp.org/www-project-internet-of-things/

Tour Eria
5 rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr