Chapitre 2
Risques et solutions

1. Introduction

Une multitude de risques et de limites existent dans le monde de l'Internet des Objets tels que la complexité d'un système beaucoup trop hybride, des réseaux de communication très hétérogènes, une absence de normes, une difficulté de relever et corriger les bugs le plus rapidement possible… Les acteurs de terrain vont être la clé, en mesure d'opérer le plus rapidement possible le débogage. Le recours à des entreprises de conseil, d'audit et de formation permet de mieux maîtriser ces risques et de profiter des opportunités de l'Internet des Objets.

Il est important « d'intégrer la notion de risque : dans une démarche d'innovation IoT, les échecs font partie du processus », précise David Gautier et Franck Nassah, les auteurs du livre blanc *IoT : quelle réalité pour le secteur industriel en France*, CXP Group, mars 2016 (p. 6).

Néanmoins, mieux les connaître permet d'en diminuer drastiquement le nombre et leurs effets.

L'étude *Navigating the Internet of Things* du cabinet VDC Research, indique que **« seuls 27 % des professionnels du secteur pensent que les objets connectés sont peu ou pas vulnérables aux attaques extérieures »**.

A contrario donc, 73 % estiment que les objets dits connectés sont quelque peu vulnérables (52 %), très vulnérables (19 %) ou extrêmement vulnérables (2 %) (source : Etude *Navigating the Internet of Things*, VDC Research, ubm.com, Avril 2013. http://www.prnewswire.com/news-releases/ubm-tech-and-vdc-research-to-unveil-navigating-the-internet-of-things-report-at-design-west-202349051.html). Quant à la toute dernière étude d'Extreme Networks sur l'IoT, elle révèle que 57 % des personnes interrogées se disent inquiètes quant à la sécurité desdits objets.

« Notre esprit ne fonctionne pas du tout comme une caméra ou une machine : toute perception est une création » (Olivier Wolf Sacks, Un anthropologue sur Mars, 1995). Une perception ne reflète pas la réalité, mais seulement un ressenti humain d'une situation. Il y a parfois un fossé, entre réalité et perception. Néanmoins, une telle perception négative sur la sécurité des objets connectés prend forcément sa source dans une certaine réalité.

Quelle est alors la réelle vulnérabilité de l'Internet des Objets en 2018?

Selon les évaluations réalisées par Digital Security en 2017 sur 100 solutions IoT, tant d'un point de vue matériel que logiciel, l'écart entre les besoins réels et les mesures de sécurité mises en œuvre est vertigineux.

Mais quelles sont alors les cinq principales vulnérabilités des objets connectés?

– Des mises à jour non sécurisées.

– Une utilisation de clés et de mots de passe par défaut.

– Un stockage de données en clair sans aucun chiffrement.

– Un accès aux interfaces de débogage ouvrant la voie à une prise de contrôle

Source : https://www.digital.security/fr/sites/default/files/imce/documents/cp-digital-security_evaluationiot-20170725.pdf

2. Les risques sécuritaires

« Beaucoup d'entreprises et d'industriels n'ont absolument aucune expérience avec la sécurité, souvent trop concentrés à fabriquer des produits, à rechercher les profits. La cybersécurité n'est donc absolument pas la priorité pour bon nombre d'entre elles », précise James Lyne, Directeur monde de la recherche sur la sécurité de Sophos, société spécialisée dans l'édition de logiciels et d'applications de sécurité. Source : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201605_en.pdf).

Pour Ismael Toure, Head of Production and Infrastructure, interviewé fin 2016, « les objets connectés ne représentent pas réellement un risque pour le particulier mais peut représenter un risque important pour les entreprises, notamment pour celles ayant une forte exposition médiatique ou concernées par des affaires ou des dossiers un peu complexes » (source : Ismael Toure, Head of Production and Infrastructure, Entretien du 16 novembre 2016 réalisé par Nicolas Préteceille, Paris).

Les risques à même de limiter la croissance de l'Internet des Objets sont nombreux et protéiformes :

– la sécurité physique et digitale des objets et dispositifs,
– la protection des données à caractère personnel ou stratégique, et donc le risque juridique et financier conséquent,
– le cadre législatif (notamment le RGPD),
– l'impact environnemental,
– les risques sanitaires,
– la problématique des grands industriels inhérente au cycle de déploiement,
– la multiplicité des produits,
– le manque d'homogénéité des réseaux,
– l'inutilité programmée des objets gadgets.

2.1 Intrusion et collecte de données

La collecte des données est probablement l'une des plus importantes problématiques à laquelle doit et devra faire face l'IoT, dans un souci de transparence et de sécurité. La CNIL et l'Europe s'emparent de plus en plus de cette problématique, notamment via l'entrée en vigueur, le 25 mai 2018, du Règlement Général sur la Protection des Données dit RGPD.

Comme le précise Vincent Strubel de l'ANSI (Agence Nationale de la Sécurité des Systèmes d'Information), dans son dernier rapport intitulé Cybersécurité des objets connectés, lesdits objets sont « **des cibles de choix pour la captation de données** » (http://cedric.cnam.fr/workshops/iot-cybersecurite-cyberdefense/Presentation_ANSSI.pdf).

2.1.1 Les différentes typologies de risques

On peut noter la manipulation de données sensibles à haute valeur comme les données à caractère personnel (données personnelles et données de santé), les moyens de paiement (numéros de cartes bancaires) ou encore, l'identité numérique d'une personne.

Ces données sont soit stockées localement, soit transmises à un tiers sur un cloud pour conservation et/ou traitement. Dans les deux cas de figure, ces données sont vulnérables. Des hackers sont dès lors en mesure de pénétrer dans les objets et dispositifs connectés avec pour finalité, le vol de données personnelles des utilisateurs.

L'autre point relativement peu évoqué est le détournement de l'usage traditionnel initialement prévu des capteurs intégrés que sont la caméra, le micro ou encore l'accès au réseau.

La manipulation de données sensibles, comme le détournement de l'usage prévu des objets connectés, peut avoir « **des conséquences potentiellement dramatiques en cas de sabotage** » comme le souligne Vincent Strudel (http://cedric.cnam.fr/workshops/iot-cybersecurite-cyberdefense/Presentation_ANSSI.pdf).

De nombreux exemples commencent à apparaître dans la presse, comme le détournement de voitures connectées, l'accès à un pacemaker ou d'autres objets connectés à usage médical en mesure d'agir sur la vie humaine de l'utilisateur.

L'usage de plus en plus important des objets connectés dans des infrastructures critiques, assurant la protection des biens ou des personnes (caméras, serrures…), nécessite de s'assurer de la parfaite sécurité et innocuité desdits objets, au regard du risque qu'une intrusion ou une utilisation malveillante puisse être effectuée.

Comme le soulignait le Premier ministre Manuel Valls dans le rapport *Stratégie Nationale pour la sécurité du Numérique* (https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf p.3), « répondre aux enjeux de sécurité du monde numérique est un facteur clé de succès collectif ». Or, Vincent Strubel, dans son rapport, indique que les objets sont globalement peu supervisés par les entreprises. **« Peu ou pas de mises à jour de sécurité, de détection des attaques et des objets peu surveillés »**, découlant sur un possible accès physique à l'objet par des attaquants aux conséquences potentiellement dramatiques.

De façon générale, aujourd'hui encore, les entreprises allouent peu de ressources pour la sécurité des objets connectés dont le niveau de sécurité est pourtant très faible. Par exemple, lors de l'envoi de données sensibles vers un cloud, le niveau de sécurisation est généralement très faible (authentification et encryptage simples).

2.1.2 La sécurité et la protection des données personnelles

La Commission Nationale de l'Informatique et des Libertés, la CNIL, est en charge de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Elle s'est emparée du sujet dans sa *lettre innovation et perspective n°4*. Elle déclare en effet que « ces nouveaux objets et services créent et stockent (souvent en ligne d'ailleurs) de nouvelles données personnelles et tracent nos activités quotidiennes, dont certaines assez sensibles, et cherchent à créer de la valeur par différents modèles économiques qui sont loin d'être neutres sur le plan de l'exploitation et de l'agrégation de données » (source : https://www.cnil.fr/sites/default/files/typo/document/Lettre_IP_N4.pdf, p. 4).

2.1.3 Les préoccupations sécuritaires

Le second élément pertinent à noter dans cette étude *Navigating the Internet of Things* de VDC Research, est le classement alarmant des préoccupations majeures des entreprises qui conçoivent des objets connectés ou utilisent l'Internet des Objets, en interne ou en externe.

En effet, **arrive en tête dudit classement des préoccupations majeures, l'aspect coût de développement et d'utilisation dudit objet, puis seulement en seconde position, l'aspect sécuritaire, pourtant capital!**

Pour que l'Internet des Objets soit éventuellement incontournable pour toutes les entreprises et qu'il puisse représenter une opportunité et non une menace, il est crucial que cet aspect sécuritaire soit au cœur des préoccupations des concepteurs et des utilisateurs. Car profiter des opportunités n'est possible que si les risques sont minimisés.

Suivent ensuite la volonté d'une mise sur le marché, ou l'utilisation et l'exploitation rapide du ou des objets, et enfin l'optimisation des performances de l'entreprise.

Selon une autre étude, à savoir celle de Hewlett Packard intitulée *Internet of Things – Research study*, il convient de mettre en évidence l'insuffisance d'authentification et d'autorisation, le manque d'encryptage lors de l'échange d'informations et des interfaces web softwares et firmwares (microcode logiciel doté de la faculté de piloter le matériel auquel il est associé) insuffisamment sécurisées.

Source : Etude *Internet of Things Research study*, Hewlett Packard, 2015, p.5. https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-4759ENN.pdf