WAVESTONE

OBJETS CONNECTÉS
LES 4 DIMENSIONS DE LA SÉCURITÉ

COMME TOUTE RÉVOLUTION TECHNOLOGIQUE, LA TRANSFORMATION NUMÉRIQUE IMPACTE DE NOMBREUX DOMAINES DE L'ÉCONOMIE : LA DOMOTIQUE, LA SÉCURITÉ PHYSIQUE, LA MOBILITÉ, LA SANTÉ, ETC.

L'Internet des Objets (IoT en anglais) joue un rôle important dans cette tendance, avec l'émergence de nombreux objets connectés. Les chiffres sont en effet significatifs : de nombreux analystes considèrent qu'il y aura entre 20 et 200 milliards d'objets connectés d'ici 2020.

AU CŒUR DE LA TRANSFORMATION NUMÉRIQUE

Aucune industrie ne peut aujourd'hui ignorer cette tendance et les entreprises voient un intérêt grandissant à s'emparer de ce qu'elles perçoivent comme une véritable opportunité.

Alors que des start-ups conçoivent chaque jour des dispositifs intelligents, des partenariats se mettent en place entre les vendeurs et les industries traditionnelles – tels les secteurs de l'assurance, automobile, administratif, bancaire – afin d'offrir de nouveaux services aux consommateurs grâce à divers éléments connectés.

UNE SURFACE D'ATTAQUE DE PLUS EN PLUS EN PLUS VASTE POUR LES CYBERCRIMINELS

L'essor de cet Internet des Objets n'est pas sans danger, d'autant plus que les risques, qui étaient surtout virtuels, s'étendent au domaine du physique.

Une étude frappante a été menée par HP Fortify[1] en 2014, mettant en avant un constat sans appel : en testant la sécurité des 10 des objets connectés les plus en vogue du moment, une moyenne de 25 vulnérabilités par objet a été trouvée. La plupart d'entre elles sont liées à des problèmes de sécurité basiques, tels que la **mauvaise gestion de la confidentialité des données et des droits d'accès**, **l'absence de chiffrement des flux**, **une interface d'administration Web non sécurisée**, ou encore **une protection générale inadaptée**.

AUTEUR

CHADI HANTOUCHE
chadi.hantouche@wavestone.com

Ce manque de durcissement augmente le risque de vulnérabilités pouvant affecter toute sorte d'objets : des réfrigérateurs aux toilettes connectées, en passant par les voitures et les serrures (voir encart ci-dessous).

DE LA SCIENCE-FICTION À LA RÉALITÉ

En 2013, la série « Homeland » a mis en scène une attaque à distance sur le pacemaker connecté d'un politicien. La même année, un ancien vice-président des États-Unis, Dick Cheney, déclarait avoir fait désactiver les fonctionnalités de contrôle à distance de son appareil cardiaque, afin d'éviter tout risque d'attaque.

En juillet 2015, deux chercheurs en sécurité sont parvenus à prendre le contrôle total d'une Jeep Cherokee, incluant les possibilités d'activer ou de désactiver les essuie-glaces, de suivre la position GPS du véhicule, voire même d'arrêter le moteur. Ce fait d'armes a conduit au rappel de plus d'un million de véhicules par Fiat-Chrysler et à la mise en place de commisions de recherche sur la sécurité automobile par le Sénat américain et par des régulateurs.

DANS QUELLE CATÉGORIE DE RISQUES VOUS SITUEZ-VOUS ?

En ce qui concernent les entreprises, les risques dépendent de la posture adoptée. Dans le cas des objets connectés, quatre cas sont possibles. Les différentes postures ont été réunies sous l'acronyme « **CARA** » (pour **Concevoir**, **Acquérir**, **Recommander**, **Accueillir**) comme le montre le tableau ci-dessous. Une fois la posture identifiée, il convient de spécifier les risques génériques et les recommandations associées.

UN OUTIL D'ÉVALUATION EFFICACE : LA MATRICE « HEAT MAP »

Afin d'évaluer le risque, le cabinet Wavestone a développé un outil spécifique, la matrice « heat map ». Elle prend en compte deux dimensions : le niveau de risque et la posture.

La page suivante présente l'exemple concret de l'utilisation d'objets connectés pour le secteur bancaire et ses divers services. Ce contexte présente des contraintes particulières. D'un côté la réalisation d'une transaction financière est plus risquée que la consultation du solde bancaire. Mais d'un autre côté, la personnalisation des fonctions de sécurité sur un appareil appartenant à un employé ou à un client est bien plus compliqué que le durcissement d'un produit choisi par l'entreprise et qui a été acquis à un fournisseur, ou même développé en interne.

Cette matrice permet de réaliser une cartographie des risques qui requièrent la plus grande attention.

La méhode CARA développée par Wavestone procure des recommandations pour chaque contexte

	Périmètre	Risques génériques	Recommandations principales
CRÉER	Les entreprises concevant des objets connectés doivent dans ce cas intégrer la sécurité dès la conception	Des failles de sécurité pourraient mettre en danger les utilisateurs ou leurs données, et donc engager la responsabilité ou nuire à la notoriété du fabricant	Intégrer la sécurité dans les phases de design, en particulier vérifier la possibilité de faire des mises à jour tout au long du (potentiellement long) cycle de vie de l'objet
ACQUÉRIR	Les entreprises acquérant des objets connectés dans le but de les déployer en interne	L'intégration de ces nouvelles technologies au sein du processus métier sans une sécurité adaptée pourrait augmenter les points d'entrées pour attaquer le système d'information	Garantir une bonne gestion de l'identité des dispositifs Demander au fabricant un renforcement de la sécurité adéquat
RECOMMANDER	Les entreprises recommandant ou offrant des objets connectés à leurs clients peuvent porter une responsabilité	La fuite de données (potentiellement personnelles) ou une atteinte à leur sécurité physique pourrait nuire à l'image de l'entreprise	Définir clairement la responsabilité (ainsi que l'appartenance des données) Garantir la conformité S'assurer que les objets recommandés ont un niveau de sécurité suffisant
ACCUEILLIR	Les entreprises pratiquant le BYOD, ne pourront pas faire l'impasse sur la sécurisation des données professionnelles ou de l'accès aux SI depuis ces terminaux	La perte ou le vol d'objets connectés pourrait mener à la diffusion des données auxquelles ils avaient accès ou faciliter une intrusion dans le SI	Sensibiliser les utilisateurs sur leurs responsabilités Améliorer la charte utilisateur Réutiliser les projets BYOD précédents

DES DISPOSITIFS DE SÉCURITÉ HABITUELS : DE NOUVEAUX MODES D'IMPLÉMENTATION

Une fois la cartographie des risques établie, il faut s'intéresser aux réponses que l'on peut y apporter. Une référence intéressante à ce propos est celle de l'initiative « IoT Project » de l'OWASP (Open Web Application Security Project – organisation à but non lucratif) qui propose notamment une liste de recommandations de sécurité intéressantes et compréhensibles[2].

La première chose à noter à propos de ce guide est qu'il est divisé en 3 catégories selon les cibles d'audience visées : fabricants, développeurs, consommateurs. Cette structure a du sens dans la mesure où **la sécurité est partagée entre ceux qui conçoivent les composants** (matériel ou logiciel), **et ceux qui les utilisent**.

Par ailleurs, les dispositifs de sécurité doivent être **complets – renforçant non pas les seuls objets connectés, mais aussi toute la surface d'une attaque** (physique, matériel, logiciel, base de données, local ou à distance, etc.). À cet égard, les mesures de sécurité proposées sont surtout construites sur les bonnes pratiques de l'industrie de la sécurité.

L'Internet des Objets apporte un réel changement dans la mise en œuvre des dispositifs de sécurité.

En effet, plusieurs contraintes liées aux objets connectés sont à prendre en compte :

- **Ergonomie :** la taille et le design influenceront les mesures de sécurité acceptables par les utilisateurs – par exemple, la taille de l'écran pour taper un mot de passe.
- **Puissance :** les petits objets embarqués actuels ont une puissance de calcul limitée. Plusieurs opérations ne peuvent être réalisées en même temps dans un laps de temps raisonnable. Par exemple, Apple a conseillé aux développeurs de ne pas implémenter des fonctionnalités nécessitant de long temps d'exécution sur l'Apple Watch.
- **Connectivité :** l'Internet des Objets utilise généralement du Bluetooth ou des protocoles NFC, deux technologies ayant une portée et un débit limité, ce qui ne permet pas toujours d'embarquer un niveau de sécurité suffisant.
- **Durée de vie de la batterie :** les algorithmes cryptographiques (comme du chiffrement / déchiffrement asymétrique en temps réel) peuvent affecter durement la consommation énergétique, même s'ils permettent de procurer un meilleur niveau de protection.
- **Gestion des mises à jour :** il est indispensable de mettre à jour le système, sans interférer avec l'utilisation de l'objet. Cela est particulièrement frappant dans le cas des voitures connectées que l'on ne peut pas conduire lorsque le logiciel est en train de se mettre à jour. Cela peut prendre plus de 45 minutes.

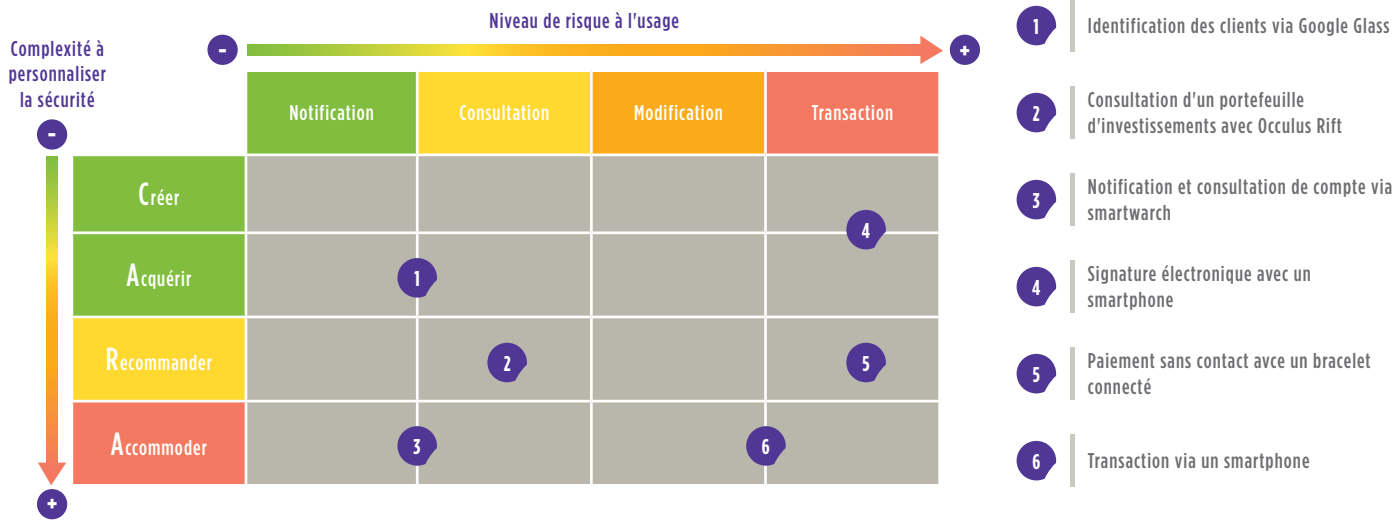
Au-delà de la sécurité, la confidentialité est également indispensable pour les consommateurs ainsi qu'une exigence pour les autorités. L'implémentation pourrait être complexe, mais plusieurs initiatives pour la confidentialité des objets connectés ont émergé ces dernières années.

Parmi ces initiatives, le projet PRESERVE[3] est un exemple intéressant. Il offre à l'industrie automobile un nouveau moyen d'utiliser les PKI et les certificats numériques pour les voitures et les routes connectées. Le projet utilise des « pseudonymes » modifiés régulièrement afin de garantir que le conducteur reste anonyme tout en assurant que les communications entre les véhicules et l'infrastructure routière sont authentiques et sécurisées.

Nous sommes entrés dans une ère où sécurité et confidentialité des données sont devenues des critères essentiels dans le choix des consommateurs. **Cette évolution ne peut plus être ignorée par les acteurs concernés, qu'ils conçoivent, acquièrent, recommandent ou accueillent des objets connectés**.

Source 1 : http://go.saas.hp.com/fod/internet-of-things
Source 2 : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
Source 3 : https://www.preserve-project.eu/

Exemple de matrice heat map pour un contexte bancaire B2C



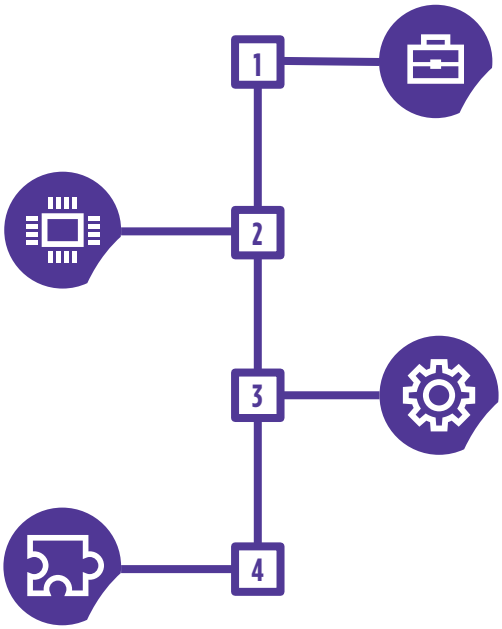
COMMENT SÉCURISER L'INTERNET DES OBJETS ?

Clarifier les cas d'usages

Les risques liés aux objets connectés peuvent dépendre de l'usage et de la posture de l'entreprise (CARA). De plus, suivant l'industrie, les objets ne seront pas utilisés de la même façon.

Prendre du recul lors de l'implémentation

Il est important de ne pas négliger l'environnement dans lequel évolue l'objet connecté ainsi que ses caractéristiques propres : ergonomie, puissance, connectivité, autonomie et surtout possibilité de mise à jour du dispositif.



Échanger avec les métiers concernés

Il est primordial de comprendre les enjeux métiers sur l'ensemble du cycle de vie de l'objet connecté, ce qui permet d'expliciter et d'anticiper les risques potentiels.

Analyser le marché et les plateformes

Deux objets relativement similaires peuvent ne pas être sécurisés aussi bien l'un que l'autre. Il devient nécessaire d'identifier les spécificités des plateformes et les limites associées.

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods). Il figure parmi les leaders indépendants du conseil en Europe.

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.