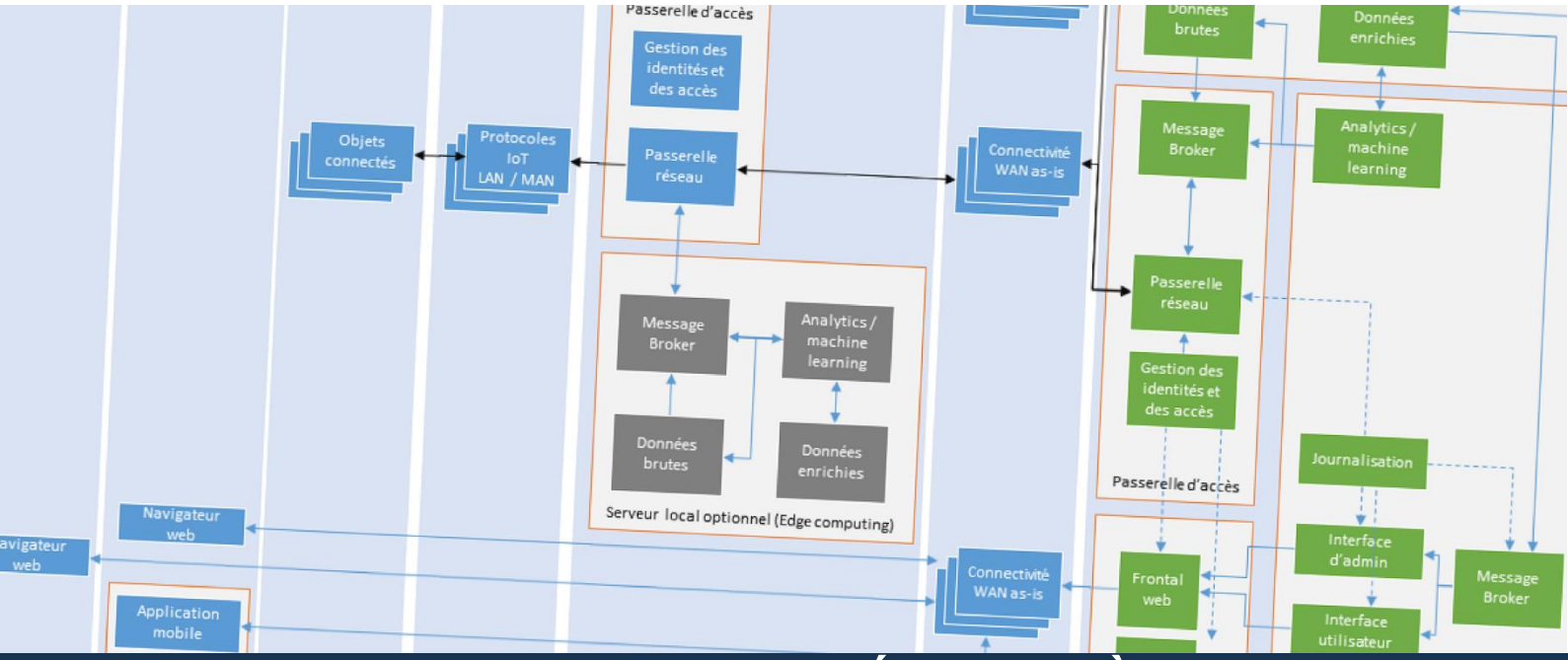
LES FICHES PRATIQUES du CLUSIF - IoT



QUI SONT LES ACTEURS DE L'ÉCOSYSTÈME IOT ?

Version 1.0

1. UN CASTING TRÈS VARIÉ

Sous le terme IoT, on regroupe de nombreuses technologies hétérogènes et des usages pour le moins différents. Cette fiche présente quelques cas d'école pour essayer d'en extraire des tendances.

Commençons par le chef de produit d'une "bouilloire connectée" ; ambiance startup et innovation, la sécurité n'est tout simplement pas une préoccupation pour lui.

L'équipe de conception technique d'un objet de fitness (balance connectée, ceinture pectorale, ou wearable…) se focalise sur les fonctions et la valeur apportées par l'objet à ses utilisateurs ; elle a principalement des contraintes de délai et de coût fortes, imposées par le marché.

Le développeur (« codeur ») d'un composant qui s'insère dans un système de gestion de flotte automobile doit respecter les délais et fonctionner dans un système contraint, voire un système de systèmes sur lequel il n'a souvent pas la main.

L'assembleur d'un thermostat connecté définit des exigences pour ses fournisseurs (composants, logiciels, Cloud, chaîne logistique…) ; conscient des enjeux, il assure la cohérence globale de la chaîne de sécurité mise en place mais ne peut pas non plus y consacrer la majorité de son temps (ni de son budget).

Le responsable de la sécurité du boîtier de surveillance qu'un assureur automobile implante dans les véhicules a des contraintes légales et juridiques fortes ; il considère principalement les risques de fraude mais pourrait aussi devenir une porte dérobée pour attaquer le véhicule ou son conducteur si le niveau d'intégration augmente.

Le RSSI du fabricant qui va mettre sur le marché un pot de fleur connecté doit intégrer l'infrastructure associée (DB, Cloud...) dans son SI ; il doit guider l'équipe innovation sans devenir un frein à l'innovation et s'assurer de la pérennité des choix.

Le DPO de l'entreprise qui va fournir un boîtier de surveillance automobile devra souvent calmer les ardeurs de l'équipe innovation ; on ne peut pas faire n'importe quoi sous prétexte que c'est techniquement possible et financièrement rentable.

L'intégrateur d'un système de gestion de la disponibilité de bureaux et de salles de réunions répond aux exigences de sécurité de ses clients ; il gère un système complexe qui devra pouvoir évoluer dans le temps (5, 10, voire 15 ans…) pour s'adapter aux nouvelles menaces.

Le RSSI d'une entreprise qui achète un système de gestion connectée des salles de réunions doit formuler des exigences de sécurité raisonnables et s'assurer de la conformité des solutions retenues. Elles doivent pouvoir communiquer avec le plus de transparence possible, mais simultanément ne pas générer d'effet de bord sur les systèmes en place.

Un agriculteur qui automatise progressivement son activité (drones, assistance par satellite, capteurs...) voit que les objets connectés deviennent centraux et vitaux pour son activité ; il n'a pas conscience des risques mais considère que la sécurité va de soi et que ses fournisseurs en ont nécessairement tenu compte.

Le maire qui veut faire l'acquisition d'un système de gestion intelligente des places de parking de sa ville a besoin de rédiger un cahier des charges détaillé raisonnable ; son investissement doit se faire sur le long terme. L'IoT s'accompagne aussi parfois d'open data qu'il faut alors encadrer.

Enfin, les citoyens/consommateurs sont autant d'acteurs complémentaires qui utilisent de plus en plus d'objets connectés, à des fins très diverses qui justifient des politiques de sécurité profondément différentes : un capteur d'eau dans un pot de fleur n'a clairement pas les mêmes contraintes qu'un pacemaker ou qu'une voiture connectée.

Au final, on peut distinguer deux grandes catégories d'acteurs : les fabricants (« Builders ») et les utilisateurs (« Buyers »), dont les priorités sont naturellement souvent différentes.

2. LES FABRICANTS

Les fabricants peuvent être fournisseurs de matériel, éditeurs de logiciel, intégrer une solution IoT à partir de composants tiers, voire fournir le service associé, souvent sous la forme d'une plateforme dans le Cloud. Les priorités des fabricants sont liées à plusieurs facteurs :

- Le coût, qui doit rester minimal pour être compétitif ;
- La disponibilité de la solution sur le marché ; il ne faudrait pas qu'elle tombe en rupture de stock !
- La capacité à passer à l'échelle ; l'idéal serait un service qui suive une progression linéaire, quel que soit le nombre d'utilisateurs, voire qui profite d'économies d'échelle ;
- L'identification des objets, pour pouvoir y associer les données collectées, et réaliser des traitements d'analyse à valeur ajoutée ;
- La préservation de l'image de la marque ; le fournisseur du service ou de l'objet final sera celui dont l'image souffrira le plus si un problème survient, même si la responsabilité incombe à l'un de ses sous-traitants.

3. LES UTILISATEURS

Les utilisateurs peuvent avoir plusieurs profils : entreprise, collectivité, artisan, PME, ou « simple » particulier, consommateur d'objets à son domicile ou en mobilité. Les priorités des utilisateurs convergent sur plusieurs dimensions :

- Le prix, directement lié au coût évoqué précédemment : l'IoT est un marché très concurrentiel et qui obéit aux lois « normales » du marché ;
- La fiabilité au sens large, mais avec un niveau de sensibilité qui dépend du profil d'utilisateur, de sa sensibilité aux questions de sécurité, et également du contexte d'utilisation : concrètement, la fiabilité se traduit en disponibilité et en intégrité du fonctionnement ;
- Le respect de la confidentialité de l'information a de plus en plus tendance à être considéré séparément, associé à une maturité croissante des utilisateurs, et à un contexte réglementaire de plus en plus contraignant.

ⓘ Point de vue du RSSI

En 2019, beaucoup de RSSIs considèrent l'IoT comme un sujet émergent qui deviendra une priorité dans quelques années. Cependant, il est probable que des projets IoT soient déjà initiés dans leur entreprise, avec un focus sur l'innovation, et que ces incubateurs n'aient pas intégré de contraintes de sécurité fortes dans leurs phases initiales car elles apparaissent plutôt comme des inhibiteurs à la créativité. Le RSSI doit donc commencer par identifier s'il est plutôt utilisateur ou fabricant, voire les deux.

L'expérience passée (par exemple dans les développements logiciels) a montré que la dette de sécurité s'accumule et qu'il faudra la payer un jour. Autant s'en soucier dès le départ et partir sur de bonnes bases. Avec l'Internet des Objets, le RSSI peut donc jouer un rôle de communicant et de sensibilisation. Il peut insuffler un ensemble de bonnes pratiques dans les projets : l'importance des mises à jour logicielles, la nécessité de signer ces patches, l'évolution régulière des menaces et le besoin de prendre en compte l'existence de failles de sécurité inconnues au moment de la création de l'objet, le contrôle des APIs qui favorisent l'interopérabilité mais qui peuvent devenir autant de portes ouvertes dans des systèmes mal sécurisés…

LES FICHES PRATIQUES

L'intégralité de la FAQ IoT et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF