Sécurité IoT : une priorité des entreprises et des opérateurs

Le niveau de sécurité, une problématique à adapter à chaque cas d'usage.

Tout d'abord, le niveau de sécurité doit être étudié en fonction du cas d'usage et être adapté en fonction du niveau de risque encouru : le risque est plus faible lors d'une simple remontée d'information et plus élevé lorsqu'il s'agit de contrôle-commande (prise de contrôle à distance). Par exemple, une simple remontée d'information de température dans une salle pour des besoins d'optimisation énergétique ne représente pas le même risque qu'un pilotage de vanne à distance.

Le choix de la technologie peut déjà induire un niveau de sécurité spécifique. Par exemple, sur les réseaux dits « bas débits, basse consommation » comme les réseaux LoRaWAN, la plupart des usages sont informatifs (remontée d'information uniquement) et les données cryptées, ce qui limite les dangers. Mais, la sécurité doit s'étudier de bout en bout, afin d'éviter toute faille dans le système.

Une sécurité de bout en bout

Il est impossible de fournir une sécurisation performante de l'IoT sans avoir une vision globale de la solution : du capteur à la plateforme applicative, en passant par les infrastructures réseaux.

La sécurisation passe d'abord par celle des capteurs, à la fois dans leur conception et dans leur installation. Ils doivent tout d'abord être conçus par des experts, et produits avec des composants de qualité. Pour renforcer leur sécurité dans les usages les plus critiques et limiter l'accès aux ports de connexions directs au capteur, on y place un « secure element », qui sera nativement intégré au hardware. Il ne faut pas non plus oublier d'installer les capteurs selon les règles de l'art ! Il faut s'assurer qu'ils soient bien positionnés et fixés, voire dissimulés au besoin.

Ensuite, le choix du protocole de communication est prépondérant car il peut y intégrer ou non une couche de sécurité grâce à un chiffrement natif de l'intégralité des messages échangés. Par exemple, dans le cas particulier de LoRaWAN, les données sont cryptées de façon native en AES128, algorithme cryptographique actuellement le plus utilisé et le plus sûr. Le protocole LoRaWAN intègre donc une couche de sécurité par défaut avec un mécanisme de gestion des clefs de chiffrements.

Également, avoir recours à un réseau qui ne soit pas directement accessible en IP, évitant un rapport direct avec internet, est un facteur de sécurité supplémentaire.

La sécurité, une affaire d'opérateur

Aujourd'hui, les opérateurs télécom IoT sont résolument engagés dans une démarche de sécurité croissante. Ils utilisent notamment des coffres-forts électroniques pour héberger les clefs de cryptage, offrant une protection de niveau équivalent à celle du monde bancaire. Dans le cas du réseau LoRaWAN Objenious, les clefs de chiffrement sont hébergées dans un système de sécurisation de clefs (KMS pour Key Management Server) fourni par les acteurs spécialistes de ces systèmes.

En utilisant des infrastructures déjà présentes comme les datacenters ou backhauls national (réseau intermédiaire utilisé pour les données GSM, fibre ou ADSL) hautement sécurisés, le degré de sécurité est encore renforcé pour éviter notamment un piratage des Métadonnées utilisées par le réseau pour la gestion de la qualité de service.

Les opérateurs opérant un seul réseau global avec un cœur de réseau unique ont également la capacité à intervenir rapidement sur l'ensemble du réseau pour corriger d'éventuelles failles de sécurité.

Malgré tout, le risque est toujours présent et dans ce paysage complexe, savoir à qui incombe la responsabilité des incidents de sécurité ou de sûreté d'un objet n'est pas toujours chose facile. Dans un premier temps, les opérateurs IoT doivent mettre en place des outils de supervision pour reconnaître un trafic de données anormalement élevé ou inhabituel. L'application d'algorithmes de machine learning peut également être d'un précieux secours dans la détection des anomalies.

Il est aussi nécessaire de mener des audits de sécurité par des cabinets experts, régulièrement ou à chaque modification des plateformes d'accès aux données IoT.

Ces principes sont des standards pour les opérateurs Télécom qui doivent assurer la sécurité des utilisateurs de ses solutions et offrir aux acteurs industriels la sécurité nécessaire au bon déroulement de leur activité.

La sécurisation des déploiements à grande échelle

Mais les déploiements à grande échelle peuvent complexifier la tâche. Lorsque l'IoT s'industrialise, c'est tout un écosystème qui doit se mettre en place.

Exemple, la certification des objets connectés par l'opérateur ou par des acteurs indépendants permet de garantir le bon usage des clés de sécurité et le contrôle de ces objets qui accèdent au réseau.

En complément des solutions spécifiques à chaque technologie, les labels tels que le Ready2Service dans le domaine du Smart-Building (label de la Smart Building Alliance) jouent également un rôle majeur de réassurance des clients, permettant ainsi d'accélérer l'adoption des nouvelles

technologies.

Formation des experts

Enfin, l'enjeu ne se situe pas dans la sensibilisation des acteurs de l'IoT, qui ont déjà intégré la nécessité de fournir un niveau de sécurisation élevé, mais dans la formation des responsables IoT dans les entreprises. Ces derniers ont pour responsabilité de faire les choix optimaux et monter l'architecture adéquate, en fonction du niveau de risque de leurs propres cas d'usage.

Pour le moment, ces métiers étant assez nouveaux et les futurs professionnels qui vont arriver sur le marché prochainement, tout comme les responsables IoT déjà en poste, vont devoir se former assez rapidement.