Horus

Sécuriser l'IoT

Depuis le cambriolage de mon appartement l'année dernière, la question de la sécurité est au cœur de mes réflexions. Pas seulement concernant ma maison, mais plus généralement liée aux appareils compatibles IoT et aux données qu'ils transmettent.

Afin de protéger ma propriété, j'ai installé des caméras connectées par WiFi dans mon appartement pour surveiller tout mouvement pendant mon absence. Mais j'ai bien conscience que si ces caméras ne sont pas protégées contre les interférences extérieures, elles pourraient bien devenir, non pas une amélioration, mais une menace pour ma sécurité. Si un hacker avait la possibilité de s'introduire dans le système des caméras et voir l'appartement, il pourrait alors l'utiliser pour le surveiller et préparer son entrée pour les moments où personne n'est présent.

Inutile de préciser que j'ai élevé le niveau de sécurité de mes caméras, mais combien de personnes qui ne sont pas des spécialistes de ces technologies seraient prêtes à franchir les étapes nécessaires pour sécuriser leurs réseaux ? Par défaut, les paramètres mis en place par les fabricants d'objets connectés IoT sont souvent du type « admin » pour l'identifiant et « password » pour le mot de passe. Cela rend la tâche bien trop facile pour des personnes mal intentionnées qui chercheraient à accéder aux appareils domestiques. D'autant plus lorsque les barrières de sécurité sont aussi faibles et que la plupart des utilisateurs finaux n'ont ni l'envie, ni la capacité de configurer plusieurs mots de passes pour leurs différents appareils.

Chiffrement des données dans les objets connectés

Plutôt que de demander aux clients finaux de sécuriser chacun de leurs appareils en utilisant un identifiant et mot de passe spécifiques pour chaque objet connecté, je crois en un modèle alternatif plus utile, utilisant une infrastructure de sécurité centralisée capable de fournir et d'injecter des identités numériques, comme des certificats et clés électroniques dans des objets connectés.

Ces éléments sont dédiés au chiffrement automatique des données que les objets connectés envoient aux applications via le réseau. Ainsi, le lien de communication peut être sécurisé.

Chez Atos, nous avons déjà mis en place différentes solutions de sécurité dédiées aux objets IoT. L'une d'entre elles est basée sur les protocoles de la LoRa Alliance qui est utilisée pour les appareils sans fil fonctionnant sur batterie et connectés à un réseau dédié. Le protocole LoRaWAN utilise plusieurs couches de chiffrement basées sur une distribution automatique des clés permettant d'assurer la sécurité au niveau du réseau, de l'application et de l'objet lui-même. Nous déployons un serveur centralisé au sein du réseau LoRa qui gère les objets connectés tout au long de leur cycle de vie et qui crée leur identité numérique pour sécuriser les données à tous les niveaux.

En utilisant les normes LoRaWAN, nous pouvons établir un réseau sécurisé et nous assurer que seules les applications reconnues par le réseau IoT peuvent lire les données chiffrées provenant des objets.

Le déploiement croissant des objets connectés nécessite d'utiliser des solutions évolutives et hautement disponibles. Comme les produits que nous déployons sont basés sur des technologies déjà capables de supporter des milliards de transactions chaque année dans le secteur bancaire, nous pouvons gérer des centaines de transactions sécurisées par seconde pour les objets IoT.

En France, nous protégeons le réseau LoRa que la filiale de Bouygues Telecom, Objenious, a construit pour des clients tels que le distributeur Carrefour, qui l'utilise pour suivre ses conteneurs de marchandises roulants en direction des supermarchés. Notre serveur distribue les clés autorisées non seulement aux objets, mais aussi aux équipements de réseau, comme les passerelles ou les serveurs d'application, ainsi qu'aux opérateurs du réseau. Même dans l'éventualité où un hacker pouvait se connecter au réseau LoRa, il serait dans l'incapacité de déchiffrer les données qu'il trouverait sans la clé utilisée par l'appareil.

Une sécurité plus intelligente pour des technologies intelligentes

Alors que l'IoT se généralise de plus en plus, les cas d'usages se multiplient mais nous entendons assez peu parler de sécurité. Je pense que c'est une erreur : la sécurité est le facteur clé de ces cas d'usage. Sans sécurité, de nombreux « business models » basés sur l'IoT s'effondreront.

Par exemple, les voitures autonomes auront besoin de communiquer de façon sécurisée entre elles et avec les infrastructures des « smart cities » comme les feux de signalisation. Elles devront savoir quand ralentir et quand accélérer, et à quelle vitesse. Certains cas de voitures hackées alors qu'elles étaient en conduite autonomes ont déjà été reportés, avec des conséquences potentiellement catastrophiques.

Sans certificats ni identités numériques, de nombreux cas d'usages IoT ne pourront pas voir le jour. Qui monterait dans une voiture dont il n'a pas confiance ? Et pire encore, qui utiliserait un pacemaker vulnérable au piratage ?

La transformation numérique est au sommet des préoccupations de tous. Mais le jour où de nouveaux « business models » deviendront une réalité, il faudra alors se concentrer sur la sécurité et sur de nouveaux moyens de sécuriser les objets IoT et de protéger les données et la vie privée de nos clients finaux.

Vincent Kahoul
Chef de produit IoT Security

Vincent Kahoul est diplômé de l'ESIGELEC à Rouen (France). Il a travaillé pour le groupe Thales pendant 8 ans, passant du développement de logiciel embarqué à la gestion de projet technique. Il a ensuite rejoint Atos en juin 2010 en tant que chef de projet pour le déploiement d'infrastructures de confiance avant de devenir responsable des produits de sécurité IoT en mars 2011. À ce titre, il est responsable de la définition de la roadmap pour une gamme de produits IoT dédiée à la transformation numérique et à la sécurité IoT. Il gère l'équipe de développement de produits, supervise les certifications de produits (comme les Critères Communs) et apporte son expertise dans le développement commercial pour les avant-ventes.

À propos d'Atos

Atos est un leader international de la transformation digitale avec environ 100 000 collaborateurs dans 73 pays et un chiffre d'affaires annuel de l'ordre de 12 milliards d'euros. Numéro un européen du Big Data, de la Cybersécurité, des supercalculateurs et de l'environnement de travail connecté, le Groupe fournit des services Cloud, solutions d'infrastructure et gestion de données, applications et plateformes métiers, ainsi que des services transactionnels par l'intermédiaire de Worldline, le leader européen des services de paiement. Grâce à ses technologies de pointe et son expertise digitale & sectorielle, Atos accompagne la transformation digitale de ses clients dans les secteurs Défense, Finance, Santé, Industrie, Médias, Énergie & Utilities, Secteur Public, Distribution, Télécoms, et Transports. Partenaire informatique mondial des Jeux Olympiques et Paralympiques, le Groupe exerce ses activités sous les marques Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify et Worldline. Atos SE (Societas Europea) est une entreprise cotée sur Euronext Paris et fait partie de l'indice CAC 40.

Plus d'informations
atos.net

Suivez-nous