Réponse aux trois questions fondamentales de sécurité dans l'Internet des Objets

 # CONNECTIVITÉ

POSTÉ LE 17.05.18

L'Internet des Objets (ou « IoT », de l'anglais « Internet of Things ») offre de nombreux avantages aux utilisateurs professionnels comme aux consommateurs. Toutefois, revers de la médaille, il présente aussi sa part de risques en matière de sécurité. Les experts d'IDEMIA examinent les principaux enjeux de protection dans l'IoT et les réponses que peut y apporter la solution d'IDEMIA dédiée à apporter de la confiance dans l'IoT.

Force imparable redéfinissant l'usine, le bureau et la maison, l'Internet des Objets apporte un grand nombre d'avantages mais aussi un souci majeur : la sécurité. La volonté d'améliorer l'efficacité et la productivité est désormais confrontée à la crainte du piratage des appareils connectés. L'histoire le confirme, ces craintes sont bien fondées. En 2017, les attaques contre les installations IoT ont en effet augmenté de 300 % par rapport à 2016 et la moitié des entreprises qui utilisent l'IoT ont subi des fuites de données l'année dernière. Rien de surprenant, donc, à ce que la sécurité soit devenue la première préoccupation des utilisateurs en entreprise au vu de l'ampleur des conséquences d'une attaque réussie.

Les risques liés à l'ouverture des portes digitales

Une fois piratés, les caméras de sécurité et les capteurs des lignes de production pourraient être exploités dans une attaque de déni de service à grande échelle ou simplement être désactivés. Ils pourraient également infecter d'autres appareils connectés ou servir de passerelle pour infiltrer l'ensemble du système informatique d'une entreprise. De plus, les données envoyées à partir d'un dispositif corrompu pourraient être erronées et avoir des implications lourdes de conséquences, comme dans le cas de dispositifs médicaux personnels.

L'éventail des menaces est très large, à l'instar de l'utilisation des dispositifs connectés. Mais, dans l'ensemble, les inquiétudes des acteurs de l'IoT sont liés à trois questions fondamentales :

1. Comment puis-je faire confiance aux données que je collecte ?

La collecte de données est l'objectif premier de l'IoT qu'il s'agisse d'éviter d'envoyer des techniciens pour les collecter, de remplacer les agents de sécurité par des caméras ou encore de surveiller l'état de santé d'un patient sans avoir besoin de le voir en personne. Aussi différentes soient leurs applications, les besoins de garantie sont les mêmes pour toutes les formes de collecte de données : elles doivent provenir d'un appareil autorisé (et non d'un clone), elles ne doivent pas avoir été modifiées et l'appareil ne doit pas avoir été corrompu. Avec sa solution dédiée à apporter de la confiance dans l'IoT, IDEMIA apporte une réponse essentielle à ce problème en créant une identité sécurisée pour chaque appareil. Grâce à cette identité de confiance, les utilisateurs peuvent être sûrs que les données proviennent d'une source autorisée. De plus, pour renforcer leur protection, les données elles-mêmes peuvent être stockées de manière sécurisée et chiffrée pendant leur transmission grâce aux algorithmes les mieux adaptés à l'appareil et au type de connectivité.

2. Comment puis-je contrôler mes appareils à distance en toute sécurité ?

Au-delà de la simple collecte de données vient la capacité à envoyer des commandes pour modifier ou interrompre des tâches effectuées par un appareil. Il peut s'agir par exemple de fermer les conduites et vannes d'une usine de produits chimiques ou, à l'avenir, de modifier le dosage de la pompe à insuline d'un patient. Encore plus couramment, il peut s'agir d'effectuer à distance une mise à jour de programme ou de logiciel sur un appareil. Le défi consiste à définir qui peut effectuer telle ou telle opération et à s'assurer que les droits d'accès sont bien respectés. La solution d'IDEMIA garantit que les ordres et les configurations à distance sont fiables et proviennent de sources autorisées. Elle permet également à un appareil de vérifier si l'expéditeur dispose bien des droits d'accès nécessaires pour donner cet ordre.

3. Comment savoir si j'ai été attaqué ?

Qu'une attaque ait réussi ou non, les utilisateurs doivent savoir si leurs appareils ont été la cible de pirates informatiques afin de réagir. Dans cette lutte, la clé consiste à analyser régulièrement les journaux d'événements des appareils et à être à l'affût de tout changement de comportement. En effet, si l'attaque a réussie, l'appareil peut commencer à se comporter étrangement : il peut se mettre à envoyer soudainement deux fois plus de données, toutes les cinq minutes au lieu de toutes les 10 heures, avec des valeurs très différentes. Des politiques de gestion des risques doivent être mises en place pour que tout changement inattendu déclenche la sonnette d'alarme. Si l'un de ces comportements est identifié, il faut immédiatement limiter la contamination. La procédure peut par exemple contraindre un appareil à fonctionner à capacité réduite – comme pour le « mode sécurisé » d'un PC en panne –, ou simplement à s'éteindre.

En tant que leader du marché de la connectivité sécurisée dans un grand nombre de secteurs, IDEMIA aide déjà les entreprises à forger et à protéger leurs dispositifs IoT. Cette mission est essentielle car une fois que les mesures de sécurité sont opérationnelles et maintenues, les fruits de l'IoT peuvent être récoltés.