L’Internet des objets ne doit pas devenir un cauchemar pour la sécurité des entreprises

L’Internet des objets ne doit pas devenir un cauchemar pour la sécurité des entreprises

En matière d’Internet des objets (IoT), les entreprises sont laissées à elles-mêmes avec des problèmes de sécurité béants. Les objets connectés, les services et les capteurs ont un potentiel important, mais représentent un risque. Heureusement, ce risque peut être géré au niveau de l’API.

C’est ce que dit en substance Mark O’Neill, vice-président de l’innovation chez Axway. Dans un récent article publié dans le Science Technology Magazine, il presse les responsables IT de commencer à s’intéresser de plus près à la sécurité de l’IoT.
« Chaque appareil intelligent, chaque application connectée récolte des données et chaque appareil intelligent, chaque application connectée risque d’exposer ces données. Les entreprises promettant une expérience exceptionnelle avec leurs produits et services connectés à l’Internet des objets doivent tenir cette promesse avec une sécurité sans précédent. »
Il estime qu’il faut prendre en compte les implications d’une chaîne d’approvisionnement bien équipée en capteurs et appareils intelligents. « Les entreprises laissent des données sensibles dans la nature et risquent une perturbation de leur chaîne d’approvisionnement si elles ne s’inquiètent pas de la sécurité quand elles utilisent codes barres, RFID ou GPS pour surveiller le fonctionnement de leur chaîne, et quand elles connectent à Internet des fonctionnalités traditionnellement gérées derrière le pare-feu de l’entreprise. »
Le temps où « les fabricants pouvaient masquer leurs API et espérer que les hackers ne les localisent et ne les manipulent pas » est révolu, ajoute Mark O’Neill.
Il y a diverses façons de mitiger ces risques. Les portails et passerelles de déploiement d’API [« API portals » et « API gateways », NdT] sont des mesures pro-actives qui peuvent aider à sécuriser un objet connecté. « La sécurité doit être pensée au niveau de l’API », affirme-t-il [sans étonnement, puisque c’est la solution que propose Axway, NdT]. Cela permet de donner « un contrôle complet de la sécurité des appareils aux vendeurs et aux fabricants, qui est dans le monde de l’Internet des objets l’endroit le plus sûr pour gérer la sécurité… Les API peuvent être le point à partir duquel les entreprises imposent leurs politiques de protection des données et de sécurité. »
Les API Gateways « permettent aux API de recevoir des patchs virtuels, une forme de sécurité montante qui évite que le trafic malicieux puisse atteindre l’API sans modifier le fonctionnement de l’appareil. Les patchs virtuels fonctionnent sans modifier le code source de l’API et permettent de gérer les risques rapidement. »
Les API Portals « permettent aux développeurs de voir comment les appareils utilisent les API dans le temps. » Ce qui permet aux entreprises de produire des audits, utiles pour « aider à enquêter sur les attaques d’API et assurer la conformité avec les réglementations de l’industrie. » Ces données sont une nécessité absolue dans certains domaines comme la santé, ajoute O’Neill. De plus, « les entreprises utilisent de plus en plus les API pour la collaboration B2B et l’échange de données ; dans ces cas précis les enregistrements d’audits pour les API peuvent être utilisés comme des méthodes de traçage sur la façon dont les gens accèdent à l’information ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/l-internet-des-objets-ne-doit-pas-devenir-un-cauchemar-pour-la-securite-des-entreprises-39805409.htm