

IoT : les objets connectés, futur cauchemar pour les réseaux d'entreprise ?

L'Internet des objets (IoT) est ses quelque 20 milliards d'objets connectés à l'horizon 2020 (dont 6 milliards dans les environnements industriels) risquent de mettre à défi les réseaux des entreprises. Et de provoquer quelques encéphalites aux administrateurs. Bien plus que la problématique du BYOD pour les PC, smartphones et autres tablettes personnels utilisés dans un cadre professionnel pourtant pas simple à gérer. C'est du moins la vision du cabinet Gartner.

« Ayant adopté une stratégie face au Bring Your Own Device, les organisations doivent maintenant accueillir les appareils des employés et commencer à traiter les 21 milliards d'appareils IoT qui, selon nous, voudront accéder au réseau de l'entreprise », avance Tim Zimmermann, analyste et vice président au Gartner. Qui poursuit : « Que ce soit une caméra de surveillance vidéo pour un parking, un détecteur de mouvement dans une salle de conférence ou la VMC (ventillation) pour l'ensemble du bâtiment, la capacité d'identifier, sécuriser et isoler tous les appareils IoT - et en particulier les dispositifs « sans tête » - est plus difficile à gérer et sécuriser. »

Congestion du réseau

L'un des risques majeurs avec l'arrivée massive des objets connectés sur le réseau est la congestion de ce dernier. Les nouveaux arrivants pourraient bien s'appuyer sur la bande passante de 1,3 Gbit/s des routeurs Wifi 802.11ac (voire 1,7 Gbit/s pour la seconde génération) fournis par l'entreprise. Pour y remédier, aux yeux de l'analyste, les équipes IT auront tout intérêt à travailler avec les services généraux et chacune des divisions métiers de l'organisation pour identifier en amont les appareils et projets raccordés à l'infrastructure de l'entreprise et son réseau. A partir de là, à l'établissement d'établir sa politique des règles et droits d'usages des objets qui viendront se greffer sur le réseau afin d'assurer une gestion optimale sur spectre hertzien disponible entre les murs de l'organisation. Et particulièrement de repérer les indésirables ou ceux qui empruntent trop de ressources.

Une politique de gestion qui passera potentiellement par la virtualisation du réseau qui permettra de segmenter les types de connexions des objets en fonction de leurs profils et les séparer du reste du trafic. « Par exemple, propose Tim Zimmermann, le trafic vidéo de sécurité et la circulation des applications d'entreprise peuvent avoir une priorité plus élevée que l'éclairage LED. » Un vaste sujet en devenir qui risque d'arriver plus vite que les entreprises ne le souhaitent.

Lire également

[Plus d'objets connectés que de smartphones dès 2018](#)

[L'Internet des objets au service des attaques DDoS](#)

[Tor s'invite dans la sécurité de l'Internet des objets](#)

crédit photo © Photobank gallery - shutterstock