Objets connectÃ©s et sÃ©curitÃ© : Des hackers dans votre maison ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 9/2/2016 13:30:00

Lâ□□Internet des objets (IoT) est, depuis quelques annÃ©es, un secteur en plein essor â□□ une expansion qui nâ□□est pas prÃªte de sâ□□arrÃªter lÃ puisque IDC prÃ©voit que le nombre dâ□□objets connectÃ©s dans le monde sâ□□Ã©lÃ¨verait Ã 50 milliards en 2020, surpassant ainsi le nombre de PC, tablettes et smartphones rÃ©unis.

Â

Si lâ□□IoT rencontre un succÃ¨s aussi retentissant, câ□□est notamment parce quâ□□il facilite le quotidien en permettant de contrÃ´ler et dâ□□accomplir de nombreuses tÃ¢ches Ã distance et en temps rÃ©el. Cependant, un grand nombre de personnes ayant succombÃ© aux objets connectÃ©s oublient que 90 % de ces dispositifs collectent les donnÃ©es personnelles selon lâ□□IoT Research Study.

Les personnes qui en ont conscience tendent Ã penser que leurs informations sont correctement protÃ©gÃ©es, or la sÃ©curisation de ces objets connectÃ©s reste encore trÃ¨s faible par rapport Ã celle dâ□□autres appareils : une enquÃªte Capgmini a rÃ©vÃ©lÃ© que seulement 48 % des entreprises sÃ©curisent leurs produits issus de l'IoT dÃ¨s le dÃ©but de la phase de dÃ©veloppement produit.

MÃªme si les objets connectÃ©s ont rÃ©volutionnÃ© le rapport des utilisateurs Ã la technologie, ils constituent une mine dâ□□or pour les hackers qui peuvent utiliser les donnÃ©es personnelles et confidentielles Ã des fins malveillantes.

Ondrej Vlcek, Chief Operating Officer chez Avast, commente :

Â« *Lâ□□IoT va irrÃ©mÃ©diablement changer et amÃ©liorer notre qualitÃ© de vie, en nous rendant plus performants et en faisant gagner un temps considÃ©rable aussi bien aux particuliers quâ□□aux entreprises. Bien que les objets connectÃ©s soient de plus en plus prÃ©sents et nombreux dans notre quotidien, la plupart des entreprises et des ingÃ©nieurs ne tiennent pas rÃ©ellement compte de la sÃ©curitÃ©, et les donnÃ©es sont souvent transmises en clair, ce qui permet aux pirates de les voler ou de les trafiquer facilement. Plus grave encore, lâ□□Internet des objets prÃ©sent jusque dans notre sphÃ¨re la plus privÃ©e offre davantage dâ□□opportunitÃ©s aux cybercriminels de sâ□□introduire littÃ©ralement chez nous, via le rÃ©seau domestique.*

Pendant des annÃ©es, les hackers tentaient dâ□□infiltrer les PC pour rÃ©cupÃ©rer les donnÃ©es des utilisateurs, telles que des informations bancaires par exemple, ou crÃ©aient des rÃ©seaux infectÃ©s par un botnet pour contrÃ´ler les ordinateurs, envoyer des spams ou lancer des attaques par dÃ©ni de service. De la mÃªme faÃ§on, les pirates ont dÃ©jÃ commencÃ© Ã transformer les appareils domestiques connectÃ©s en â□□appareils zombies collectant les donnÃ©es.â□□ En effet, les attaques dâ□□aujourdâ□□hui sont de plus en plus basÃ©es sur ingÃ©nierie sociale, adoptant des mÃ©thodes sophistiquÃ©es ayant pour but de piÃ©ger lâ□□utilisateur en lâ□□incitant Ã installer des malware ou Ã modifier des paramÃ¨tres quâ□□il ne comprend pas vraiment.

Dans ce contexte, il en va de la responsabilitÃ© des constructeurs dâ□□objets connectÃ©s de renforcer la sÃ©curitÃ© de leurs produits afin de protÃ©ger efficacement les donnÃ©es de leurs clients, mais Ã©galement dâ□□Ã©duquer davantage les consommateurs sur lâ□□importance de la

protection de leurs donnÃ©es pour quâ□□ils soient plus vigilants dans leur utilisation.

Pour protÃ©ger sa vie privÃ©e, il faut dâ□□abord sâ□□assurer de la sÃ©curitÃ© de son rÃ©seau et de ses communications en suivant quelques rÃ¨gles dâ□□or simples et efficaces telles que lâ□□installation de solutions de sÃ©curitÃ© qui permettent de scanner automatiquement son rÃ©seau et de prÃ©venir en cas de dÃ©tection dâ□□une faille ou dâ□□une prise de contrÃ´le des appareils connectÃ©s ; cela peut Ã©viter de se faire rÃ©veiller en pleine nuit par le lancement de la machine Ã laver ou de se faire tremper par lâ□□arrosage automatique lors dâ□□une pause bronzage dans le jardin ! Enfin, il est crucial dâ□□utiliser un mot de passe unique â□□ et, si possible, complexe â□□ pour chaque service ou site en ligne, et de rester vigilant sur des rÃ©seaux Wi-Fi publics. Â»