L’Internet des Objets, Kesako ?

13/02/2019

Bonsoir le Monde !

Les objets ont leur Internet à eux ?
Ben non hein m’fi ! Quoique …

L’**Internet des Objets** représente les objets **connectés à l’Internet** (directement ou pas), le même Internet que celui que vous utilisez ainsi que votre réseau domestique (câblé ou WIFI) !
Il s’agit de tous ces brols soi-disant intelligents qui sont « connectés » ! Surtout ceux sans fil !
Frigo, machine à laver, voitures, webcams, imprimantes, smartphones, thermostats, lampes, chauffages, appareils domotiques en tout genre, smart-TV et tout et tout !
Vous avez sans doute déjà vu le sigle **IoT** qui signifie « **Internet of Things** » et qui se traduit en français par « Internet des Objets » !

Pour assurer le succès de ces machins qui communiquent aussi de plus en plus souvent entre eux, il fallait qu'ils soient bon marché et très faciles à utiliser !
On a tellement bien fait ça que le marché est en pleine expansion pour ne pas dire explosion (on prévoit du câblage domotique dans les nouvelles maisons et/ou l'usage d'interrupteurs sans fil) **mais on a oublié un truc… la sécurité !!!!**

Ce n'est pas la première fois (cf WIFI, routeurs, Windows et consorts) mais là on atteint des sommets d'inconscience (ou d'incompétence des constructeurs) !
Un complotiste dirait « je parie que c'est voulu » !
Toutes les communications en clair (y compris le stockage du mot de passe WIFI), aucune ou très peu de protection de base (même mot de passe par défaut pour tous les appareils d'un même fabricant), micrologiciel (ou micro code ou firmware) hyper-simplifié et plein de bugs jamais corrigés (la mise à jour n'est même souvent pas prévue).

Les techniques de chiffrement existent mais sont **lourdes à implémenter** dans une ampoule LED télécommandée par exemple. De plus, il existe une myriade de méthodes de cryptage (ou chiffrement) plus ou moins résistant aux techniques d'attaque et les clés qui servent à ce chiffrement protecteur doivent pouvoir être renouvelées (c'est comme pour un mot de passe).

Une autre notion est beaucoup trop souvent ignorée par ces gadgets, c'est la **protection de la vie privée** ! Les constructeurs profitent de la connexion à l'Internet pour faire envoyer tout un tas de données dont vous n'avez que faire ni la moindre idée de ce qu'elles contiennent vers la maison mère ou autre(s) sans vous demander votre avis; on justifie ça en disant que c'est pour améliorer les

produits … (ici je voulais initialement écrire « mon c.. c'est du boudin » mais je me suis retenu…)
Je ne suis pas certains que les constructeurs le fassent vraiment car il faut un investissement très important pour traiter toutes ces informations (Big Data) provenant de ces gadgets bon marché et la preuve en est que le nombre de firmes déployant de l'intelligence artificielle permettant d'analyser ce Big Data est en diminution depuis 3 années consécutives.

Comme d'hab, le législateur est et sera toujours 3 guerres en retard et les millions d'assistés que nous sommes au niveau informatique sont bien incapables de savoir comment rendre ça correctement sécurisé ! Par contre les quelques centaines ou milliers de hackers sont des pros et/ou des passionnés et travaillent depuis plusieurs années en réseau … ben oui, via l'Internet…
L'Europe a au moins tenté d'imposer le **GDPR/RGPD** qui force à demander notre autorisation chaque fois qu'il y a stockage et/ou transmission de données mais ça sert juste à nous faire prendre conscience de partout où ça se passe mais ne change rien puisque si on dit « non », le brol ne marche plus ! En plus, c'est emm…nnuyant au possible !
Une autre tentative est d'obliger les constructeurs à assurer **une garantie de 2 ans** sur tout matériel électronique même très bon marché; cette contrainte fait

qu’on jette moins vite un appareil (car il tombe moins vite en panne) et qu’il y a donc aussi moins de risque de piratage de ces appareils « connectés » qui, je vous le rappelle, contiennent des tas d’info sur vous et sur votre réseau informatique à la maison !

Comment tu dis ? Tu t’en fous ?
Ben oui, on n’a en fait pas d’autre choix pour l’instant mais il faut être conscient que mettre sa domotique en mode vacances est une bonne indication de votre absence et je ne prend ici qu’un tout petit exemple que tout le monde comprendra ! Je vous rappelle que beaucoup de ces gadgets communiquent avec l’Internet pour plein de généralement bonnes raisons mais sans trop se soucier de la confidentialité de ces communications qui sont donc susceptibles d’être interceptées sans trop de difficulté.

Je ne veux pas vous foutre la trouille ici mais je voulais attirer votre attention sur cet aspect très peu mis en avant sauf en cas de piratage massif découvert par hasard et qu’on n’a pas réussi à étouffer et qu’on oublie aussi vite (sauf évidemment quand on est concerné) !
Je vous rappelle qu’il y a beaucoup d’argent en jeu ici et en partie le vôtre !

Le risque zéro n’existe bien évidemment pas et le seul appareil informatique sécurisé, c’est celui qu’on n’allume pas !

Mais c’est qu’il nous titille la parano le P’ti Fouineu ! Salopiaud va !

Li P’ti Fouineu vous salue bien !

PS1: kesako est la forme anglaise d’un mot bien français, quèsaco, signifiant « qu’est-ce que c’est ? » (regardez donc au dico et vous verrez que je ne raconte pas que des bêtises) !
PS2: mon correcteur orthographique veut remplacer « quèsaco » par « cosaque » – En avant pour le quèsatchok ! Comment ça kekseksa ? N’importe quoi, bien sûr !


HARRY
POTTER