Sécurité et IoT : pourquoi le pire est encore à venir

Si les experts pointent depuis longtemps les problématiques de sécurité que soulève l'IoT, la récente attaque dont a été victime le prestataire DNS Dyn a fait plus pour la prise de conscience de tous que des années de discours sur le sujet. Une table ronde organisée le 26 octobre dans le cadre du salon IoT Planet de Grenoble, et faisant intervenir plusieurs spécialistes du sujet, a permis de mesurer l'étendue du problème, qui ne se limite pas aux seules attaques par déni de service. Responsable du réseau d'Objenious, la filiale de Bouygues Telecom qui déploie un réseau pour l'Internet des objets sur la base du protocole Lora, Arnaud Vandererven décrit la surface d'attaques et les possibilités s'offrant aux assaillants. Des possibilités multiples. Celles-ci vont de la corruption des objets – pour y implanter un malware, pour en réutiliser les clefs d'authentification, pour en corrompre les données… – à l'attaque DDoS visant le cœur de réseau ou ses passerelles, en passant par l'espionnage des communications, l'usurpation d'identités ou le blocage des connexions légitimes via des interférences.

« *Dès qu'on aborde des cas d'usage en entreprise, convaincre les clients que le système est sûr et sécurisé est réellement crucial. Imaginons une compagnie travaillant dans la distribution d'eau et installant des compteurs communiquant ; si le système tombe en panne, elle ne peut tout simplement plus facturer ses clients* », illustre Arnaud Vandererven. La problématique est d'autant moins simple à appréhender que les capteurs déployés doivent ne coûter qu'une poignée d'euros, afficher une durée de vie d'environ 10 ans… et sont bâtis par un grand nombre de sous-traitants.

Prévoir le 'suicide' des objets

En face des assaillants dont les motivations peuvent être diverses. La reconnaissance de leurs pairs – c'est le cas des chercheurs en sécurité notamment -, le détournement d'argent, mais aussi la création d'un climat de terreur. Andrew Patterson, le directeur du développement de la société américaine Mentor Graphics, évoque notamment le cas de la voiture connectée. Si la fameuse prise de contrôle à distance d'une Jeep Cherokee visait à alerter le public des dangers d'un manque de sécurité de ce type de véhicules – avec toutefois des conséquences financières très concrètes pour le constructeur -, ce type de vulnérabilités pourrait également être exploitées afin d'instaurer un climat de terreur. Et Andrew Patterson d'évoquer notamment des attaques DDoS contre les Lidar, ces mécanismes de télédétection par radar utilisés sur les véhicules autonomes ou possédant des dispositifs d'assistance à la conduite. « *Une forme d'attaques par déni de service contre laquelle il est très difficile de se préparer* », avertit-il.

« *L'important, c'est d'être en mesure de maintenir la sécurité durant toute la durée de vie des capteurs, via le déploiement de nouvelles clefs, de patchs de sécurité ou de mises à jour de firmwares* », dit Pierre Girard, expert en solutions de sécurité chez Gemalto. Bref se préparer à réagir. « *Dès la conception, les fonctions de détection d'incidents et de réaction aux attaques doivent être intégrées*, reprend Pierre Girard. *Comme la capacité à organiser le 'suicide' des objets connectés, leur remise sur pied et la mise à jour de leur firmware. Et ces fonctions doivent être testées et leur sécurité validée.* »

Dès le niveau du silicium

Car il semble bien difficile de prévoir tous les scénarios d'attaque ou de mettre au point une solution miracle capable de parer toutes les tentatives. « *J'aimerais vous dire que nous avons conçu une brique capable de sécuriser tous les objets, mais ce n'est pas le cas*, lance Ruud Derwig, un architecte logiciel de Synopsys, éditeur développant des services intégrés au silicium. *Sécuriser l'IoT signifie travailler sur une chaîne complète d'acteurs et de technologies, en commençant au niveau du silicium* ». Bref, un travail collaboratif, où la sécurité globale de la chaîne dépend de l'élément le plus faible, comme l'a souligné le malware Mirai, utilisé pour monter le botnet qui a ciblé Dyn notamment. La propagation de Mirai a été facilitée par les erreurs de sécurité grossières commises par certains fabricants de caméras IP et autres enregistreurs vidéo (comme des mots de passe par défaut codés en dur).

Une chaîne d'intervenants pour laquelle le coût de la sécurisation doit, qui plus est, demeurer modique, faute de quoi c'est le modèle économique de l'IoT qui s'effondre. « *Pour un fabricant (de capteurs connectés, NDLR), la difficulté se résume à bâtir un objet totalement protégé à un coût très bas*, résume Stéphane Courcambeck, expert en sécurité de STMicroelectronics. *Avec le chiffrement, la difficulté réside dans les techniques mises en œuvre pour protéger les clefs pendant toute la durée de vie du dispositif. Et il faut aussi s'assurer que ces clefs sont employées correctement, en étant très attentifs aux interfaces.* » Inutile d'espérer voir les concepteurs de systèmes embarqués et autres objets connectés se lancer dans les certifications les plus exigeantes en matière de sécurité du code. Avec ces dernières, tester une ligne de code revient à environ 10 dollars, selon Andrew Patterson. Soit le coût du capteur dans son entier dans bien des cas !

Une loi pour responsabiliser ?

Pour Pierre Girard, nous faisons face à un défi collectif : « *l'impact de l'insécurité technologique va de plus en plus ressembler à celui de la pollution. Nous devons trouver un moyen de changer les comportements pour obliger tout un chacun à agir dans le sens du bien-être de la société dans son ensemble* ». Autrement dit, une régulation qui impliquerait notamment la responsabilité des acteurs en cas de manquement à leurs obligations minimales de sécurisation. Pour Ruud Derwig, l'enjeu réside également dans la formation et les compétences impliquées sur les projets : « *en matière d'IoT, une bonne part de l'innovation provient des start-up ou de la communauté des makers. Or, ces organisations comptent souvent peu d'experts en sécurité.* »

Selon les experts, un pas a toutefois été effectué : la prise de conscience a eu lieu. « *De plus en plus, les organisations réfléchissent à la sécurité avant d'écrire la première ligne de code* », assure Andrew Patterson. Ce qui ne change rien pour le gigantesque parc d'objets connectés déjà déployés. « *Le malware Mirai n'a exploité qu'une partie des terminaux mal sécurisés*, remarque Stéphane Courcambeck. *Désormais, les hackers vont rechercher d'autres objets mal configurés. Nous n'avons d'autre choix que de compter sur les acteurs de l'infrastructure pour renforcer leurs investissements dans les infrastructures afin de résister à des attaques dont l'intensité est appelée à augmenter.* » Ce qui revient à faire reposer le coût de l'insécurité de l'IoT sur la société toute entière. Triste aveu d'impuissance.

A lire aussi :

Dyn submergé par un botnet de 100 000 objets connectés

Les hackers éthiques au secours de la sécurité de l'IoT

Des attaques DDoS de plus de 10 Tbit/s en vue ?

Crédit photo : adike / shutterstock