Les objets connectés représentent-ils un risque ? | Denis JACOPINI

Les #objets connectés représentent-ils un risque ?

Contrôler sa maison ou son appartement du bout des doigts, voici la promesse des fameux objets connectés. Des réfrigérateurs aux téléviseurs, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages… de plus en plus d'équipements du foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, encore inimaginable il y a quelques années, se cachent d'inquiétants problèmes de sécurité. État des lieux.

Un marché en ébullition

Longtemps réservée aux technophiles fortunés, la #domotique commence vraiment à se démocratiser grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Hi-Fi, imprimantes…), les appareils électroménagers connectés – réfrigérateurs, lave-linge, cafetières, réveils, etc.– commencent à débarquer sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules adaptables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvements/fumée, alarmes…), ou encore le chauffage qui rencontrent un succès grandissant.
L'embellie du marché de la domotique s'explique notamment par la simplicité d'installation et d'usage de ces nouveaux produits, mais également par leur prix de plus en plus abordable. Toutefois, comme n'importe quel appareil qui se connecte à un réseau Wi-Fi et à Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, ont été soit démontrées par des experts de sécurité, soit exploitées par des hackers. Nous verrons les cas les plus effrayants qui donnent matière à réflexion.

Des appareils sous haute surveillance

Outre les incidents révélés ici et là, la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un moteur de recherche public étonnant baptisé Shodan. Créé par un Américain du nom de John Matherly, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domotiques, que des imprimantes, des caméras, des alarmes, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore, des réacteurs.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shodan n'aurait pas été créé pour nuire, mais au contraire pour aider les experts en sécurité à identifier les vulnérabilités des logiciels et infrastructures réseau des entreprises. Le service se targue de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'en reste pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

Les promesses de la maison intelligente et connectée

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Inutile d'avoir à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domotique soi-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies au quotidien, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation…).

Confort, sécurité, prévention, économie d'énergie…

Domotique

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des serrures qui se ferment à distance, des caméras et des détecteurs de mouvements capables de s'animer en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumée (obligatoires dans toute l'Union européenne à partir de mars 2015) qui lancent des alertes en cas de départ d'incendie, des éclairages qui créent différentes ambiances lumineuses selon les heures de la journée… Les possibilités sont quasi-infinies.

Réaliser une installation domotique est maintenant à la portée du plus grand nombre grâce, notamment, à ce qu'on appelle les box domotiques. Ces systèmes prêts à l'emploi que l'on trouve dans tous les magasins de bricolage et d'électronique (Castorama, Leroy Merlin, Electro Dépôt…) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (relié au réseau Wi-Fi du foyer), et d'un éventail plus ou moins important d'équipements de surveillance, d'automatisation, de loisirs, etc.

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées.

Créer des scénarios

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, du mois, voire de l'année. Les fabricants ont réalisé d'énormes progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables au vocabulaire incompréhensible, place aux icônes visuelles, aux photomontages représentant les différentes parties du foyer, et à des menus dynamiques inspirés de ceux des smartphones. Quelques clics suffisent pour créer plusieurs scénarios pour la journée, la nuit, le week-end, et les combiner entre eux.

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques

On peut imaginer, par exemple du lundi au vendredi, un scénario qui consisterait à déclencher une série d'actions à partir de 7 heures : ouvrir les stores, allumer le ballon d'eau chaude, faire chauffer la cafetière, lancer la radio, déverrouiller les portes, démarrer les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques n'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans un domaine précis (surveillance, automatisation, éclairage, chauffage…) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, réveils intelligents, ampoules connectées…) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

Le problème, c'est que tout ce petit monde ne parle pas le même langage. Les standards universels, que rêvent de concevoir Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme la box universelle Lifedomus Vision (2 988 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (KNX, EnOcean, MyHome, Zwave, Modbus, Zigbee…), mieux vaut s'équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

Quels risques pour la sécurité ?

Depuis quelques mois, la sécurité de l'Internet des objets fait couler beaucoup d'encre. Aux quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer les vulnérabilités de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont plus seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés prouvent le bien-fondé de leurs craintes.

Failles et vulnérabilité des objets connectés

La division de sécurité Fortify on Demand du constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 10 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, webcams, boxs domotiques…). Sans donner plus de précisions sur les marques concernées, elle déclare que la plupart ne crypte pas les données échangées sur le réseau et n'exige pas de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des mots de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines interfaces Web ne sont pas du tout sécurisées.

Toujours selon ce rapport, 90 % des produits évalués collectent des informations personnelles sensibles (adresse email/postale, date de naissance…) susceptibles de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne précisant pas les modèles et les marques des appareils incriminés. À travers cette étude, la division déclare vouloir sensibiliser les acteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

Ce n'est pas la seule étude de ce type. Le groupe de chercheurs indépendant d'AV-Test avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques iComfort de REVRitter, et XAVAX MAX ! d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Aussi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau lors des mises à jour logicielle ou firmware, mais en plus, la solution iComfort ne nécessitait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, n'importe qui aurait pu repérer les dispositifs de la marque sur Internet et en prendre le contrôle à distance… Effrayant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

Le lapin Karotz sécurisé ? Pas tout à fait.

Dans la sécurité informatique, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour proposer des patchs. Certains exemples sont particulièrement croustillants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux lapin multifonctions Karotz qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son micro pour l'espionner.

Des ampoules qui éclairent et déverrouillent les réseaux Wi-Fi

Plus récemment, des chercheurs sont parvenus à prendre le contrôle d'ampoules connectées Lifx en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans un rayon de 30 mètres dans le réseau Wi-Fi domestique auquel elles sont connectées et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est empressé de publier un correctif.

Des Smart TV qui espionnent les téléspectateurs

Les démonstrations les plus impressionnantes ont souvent lieu lors des conférences Black Hat organisées chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférenciers ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

Le thermostat Nest Lab qui joue les « Big Brother »

À l'occasion de la dernière édition qui s'est déroulée au mois d'août 2014 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (uniquement), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations récoltées par l'appareil, sans que son propriétaire s'en aperçoive.

Nouvelle génération de cyberattaques

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophiste de la situation, les cyberattaques sur les objets connectés présentant des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, babyphones, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

Des caméras au service des voyeurs

Impossible de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient un an plus tard à être espionnés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

Un hack jusque dans… le berceau d'un nourrisson !

Début 2014, la société spécialisée en sécurité PenTPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des NAS, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spams (botnet) et envoyer plus de 750 000 emails frauduleux. Dans l'État de l'Ohio aux États-Unis au mois d'avril dernier, un hacker n'a rien trouvé de mieux que de pirater un babyphone pour terroriser un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, il s'est mis à hurler des insanités sur le nourrisson.

Analyse et collecte de données en règle

En Grande-Bretagne, le blogueur spécialisé en développement informatique connu sous le nom de DoctorBeet's a fait une étonnante découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme on peut en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. En cherchant à en savoir plus, il constate en effet que son téléviseur dispose d'une fonction activée par défaut de collecte d'informations de visionnage.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de scruter ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. Un scandale dont se serait bien passé LG qui aurait, depuis, décidé de permettre à ses clients de « vraiment » désactiver l'option de collecte de données. Outre le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi redoubler d'attention et se méfier des pratiques intrusives de certains fabricants !

Source DoctorBeet's Blog

Sous l'œil de Shodan

En faisant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on se rend compte qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes pouvant être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai problème, d'autant qu'avec un moteur de recherche comme Shodan, tous les appareils connectés ayant une adresse IP visible sont désormais répertoriés sur le Web.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés connue (DLink, Netgear, Samsung…) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam…) pour voir apparaître leurs adresses IP et s'y connecter. Le service indique de surcroît de nombreux détails sur les dispositifs, comme leur système d'exploitation, s'ils sont connectés, protégés ou non par des identifiants, etc.

Comme cela avait été démontré dans une enquête baptisée Null CTRL, réalisée par deux journalistes norvégiens pour le site Dagbladet en 2013, d'innombrables équipements connectés référencés par Shodan ne possèdent aucune protection. Quelques clics suffisent pour les repérer et visionner, par exemple, le flux vidéo de caméras de surveillance chez des particuliers, jouer avec le tableau électrique ou le thermostat d'un immeuble, s'introduire dans des bases de données, etc. Gageons qu'à terme, cette surexposition des objets connectés permette de sensibiliser les utilisateurs sur l'importance de sécuriser leur accès.

Qu'en pensent les experts ?

Au-delà des rapports alarmants, des exploits des chercheurs et des affaires relatées dans les médias, nous avons souhaité donner la parole à un expert en sécurité ainsi qu'à un fabricant de solutions domotiques. Tous deux apportent une vision concrète sur les risques que représentent les objets connectés à l'heure actuelle, et donnent quelques conseils aux utilisateurs pour mieux se protéger.

Cybermesures sur les maisons intelligentes

Pour en savoir un peu plus sur les menaces qui planent sur les maisons intelligentes et leurs installations domotiques, nous avons rencontré un expert en sécurité qui travaille depuis plus de dix ans pour Kaspersky Lab Angleterre. Il dresse un portrait plus nuancé que celui des cabinets d'experts en sécurité que nous avons évoqué précédemment.

David Emm

Clubic : Que pouvez-vous nous dire sur la sécurité des objets connectés pour la maison ?

David Emm : Les gens utilisent Internet pour faire des achats, gérer leurs comptes en banque, aller sur les réseaux sociaux mais aussi pour chercher des informations liées à tous les aspects de leur vie quotidienne. Et cela va encore plus loin maintenant que nous utilisons les technologies informatiques pour réaliser des actions qui étaient, par le passé, purement mécaniques, voire manuelles. Malheureusement, lorsque de nouvelles technologies voient le jour, ou lorsque la technologie génère de nouveaux usages, la sécurité n'est souvent pas l'une des priorités. Ce n'est pas un phénomène nouveau et si l'on regarde en arrière, on remarque que les évolutions sont portées par une volonté de simplicité, de réduction des coûts ou d'autres bénéfices, alors que la sécurité n'est envisagée qu'après l'émergence d'un problème. Les risques sont multiples, allant du vol à la manipulation des données. Il est facile d'imaginer par exemple qu'un compteur intelligent soit manipulé pour falsifier la consommation électrique. Pour l'instant, cela reste de l'ordre du possible plus que de celui du réel car à ma connaissance il n'y a eu aucune attaque réelle visant des compteurs électriques.

Clubic : Selon vous, quels sont les types d'appareils domotiques les plus vulnérables ?

David Emm : Lorsqu'ils entendent parler de l'Internet des objets ou de maisons intelligentes, la plupart des gens imaginent leurs appareils traditionnels disposant de nouvelles fonctionnalités (réfrigérateur, contrôle des portes, chauffage central, etc.). Pourtant, ces appareils ne sont pas encore massivement connectés et pour l'instant, leur vulnérabilité a été démontrée le plus souvent au travers d'exploits d'experts dans le cadre de tests. Bien sûr, lorsque ces appareils seront plus courants dans nos vies, je pense qu'ils deviendront régulièrement la cible d'attaques. Mais il faut surtout s'inquiéter de la vulnérabilité d'appareils qui sont aujourd'hui des incontournables, comme par exemples les modems Internet, les tablettes, les smart TV, etc.

Clubic : À quel type d'attaques les maisons intelligentes (Smart Home) sont-elles exposées ?

David Emm : Je dirais qu'il y a trois principales catégories :
1 – Obtenir l'accès à un appareil et l'utiliser pour prendre le contrôle d'autres systèmes connectés dans la maison
2 – Avoir accès à des informations privées ou sensibles, y compris des mots de passe
3 – Falsifier des informations reçues / envoyées par un appareil à l'insu des personnes du foyer

Clubic : Quelles sont les vulnérabilités que vous avez pu constater ?

David Emm : L'un de mes collègues David Jacoby a publié un rapport pour alerter sur les dangers de l'exécution de code à distance et des mots de passe faibles sur les appareils de stockage NAS, mais aussi la possibilité d'orchestrer une attaque de type « man-in-the-middle » (NDRL : l'attaque de « l'homme du milieu » consiste à s'infiltrer sans être vu dans un réseau et y intercepter des informations) via une Smart TV. Il a également découvert des fonctionnalités d'analyses non référencées intégrées dans les routeurs par les constructeurs (sans doute pour des raisons légitimes), mais qui pourraient être exploitées par un attaquant. Un appareil sans fil est repérable et potentiellement vulnérable aux attaques lorsque ses communications ne sont pas cryptées, et que le mot de passe d'accès utilisé est celui par défaut ou faible.

Clubic : Est-ce que Kaspersky envisage de proposer des solutions de sécurité pour les objets connectés ?

David Emm : Ce n'est pas parce qu'il est possible d'installer une solution de sécurité sur les terminaux traditionnels (PC, tablettes, smartphones…), que cela sera possible sur tous les appareils du quotidien qui sont connectés à Internet. Ces appareils pourraient recevoir et envoyer des données sans pour autant autoriser l'installation de code ou disposer de suffisamment d'espace pour le faire. Ils pourraient être verrouillés (par exemple si une Smart TV tourne sous un OS standard, il est possible que le code ne puisse être modifié que par le constructeur). En plus, le vendeur n'est pas toujours le constructeur des composants informatiques intégrés. Cela signifie qu'il pourrait être impossible de patcher ces appareils; même en cas de mise à jour de sécurité disponible via le constructeur des composants. On comprend mieux pourquoi il est primordial que les constructeurs et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées.

Clubic : Que peuvent faire les utilisateurs pour protéger au mieux leurs systèmes domotiques ?

David Emm : La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple…).

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

David Emm : C'est une question difficile, car LE scénario catastrophe impliquant un seul individu n'aura pas forcément le même impact au niveau d'une communauté. Pour les individus, le risque qui importe c'est le #vol de données personnelles – par exemple, les noms d'utilisateurs, les mots de passe, etc. Ou encore, le fait que l'on puisse vous espionner vous ou votre famille (comme le hack du babyphone survenu dans l'Etat de Ohio). Il y aussi le risque qu'une application contrôlant la sécurité de votre porte d'entrée puisse être hackée, vous laissant enfermé dehors. Du point de vue de la communauté, l'impact peut être plus important. Si un hacker arrive par exemple à intercepter des données d'un compteur intelligent (Smart Meter), cela peut affecter les relevés : ils peut remettre les compteurs à zéro, voire créer une panne générale d'électricité.

Le point de vue d'un spécialiste de la domotique

Pour compléter ce dossier, nous avons voulu donner également la parole à un fabricant de solutions domotiques. Somfy, l'un des leaders du marché de la domotique, a bien voulu répondre à nos questions sur la sécurité des maisons intelligentes.

Clubic : Comment la box Somfy et les appareils qu'elle permet de piloter à distance sont-ils protégés ?

Somfy : En tant que spécialiste de solutions domotiques, notre box prend en compte les problématiques de sécurité. L'ensemble des actions effectuées avec nos solutions Tahoma et Somfy Box transite sur un serveur sécurisé et est chiffré sur 128 bits. Le protocole RTS propriétaire de Somfy (10 millions de systèmes installés dans le monde) qui est utilisé pour la commande radio est sécurisé grâce à un code tournant de 16 millions de combinaisons.

Clubic : En tant que fabricant, que pensez-vous du remous médiatique autour de la vulnérabilité supposée ou avérée de certains objets connectés pour la maison ?

Somfy : Nous sommes aujourd'hui en plein boom des objets connectés, avec de nombreux nouveaux acteurs qui lancent parfois des solutions un peu trop vite et pas suffisamment abouties. Il faut veiller à bien se renseigner sur le fabricant et sa légitimité sur le secteur. Somfy possède une expertise en matière de radio et d'IP qui nous rend légitimes sur ce secteur. Depuis que nous avons lancé notre box il y a quatre ans, aucun piratage ne nous a été signalé.

Clubic : Quels sont selon vous les points faibles d'une installation, ou quels pourraient-ils être ?

Somfy : Les points faibles de l'installation seraient de ne pas avoir de système de protection, d'avoir positionné les détecteurs de mouvements aux mauvais endroits ou de ne pas couvrir tous les accès de la maison.

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

Somfy : Le scénario catastrophe, s'il y en a un, serait de se faire voler son téléphone sans code pour le déverrouiller en laissant ainsi libre accès à l'application qui commande la maison intelligente. Il faut donc prendre les précautions nécessaires.

Conclusion

En moins de deux ans, la domotique est passée d'un marché de niche à un nouvel eldorado convoité par la plupart des géants de l'industrie high-tech. Apple, Google, Microsoft ou encore Samsung, pour ne citer qu'eux, se sont lancés tour à tour sur ce marché promis à une très forte croissance en multipliant les partenariats et les rachats de start-up spécialisées. Début 2014, Google n'a pas hésité par exemple à faire la troisième acquisition la plus importante de son histoire, en rachetant Nest Labs pour la bagatelle de 3,2 milliards de dollars et, plus récemment, le spécialiste de caméras IP Dropcam pour 555 millions de dollars.

Courant 2014, Samsung s'est offert la start-up spécialisée SmartThings (montant de l'achat non divulgué), Microsoft a noué un partenariat avec Insteon, un des leaders de la domotique aux USA, et Apple a dévoilé à l'occasion de la WWDC la plateforme HomeKit pour iOS8 qui permettra de contrôler les objets connectés de nombreux fabricants via Siri (l'assistant vocal d'Apple). En attendant les solutions des poids lourds des nouvelles technologies, le marché est déjà bien occupé par les acteurs historiques – Somfy, Philips, Haier, Legrand, etc. –, une foule de nouveaux fabricants de tous horizons, des fournisseurs d'électricité ou encore des opérateurs comme Orange et SFR, qui commercialisent en France des kits de domotique pour accompagner leurs box. Si tout ce monde frappe à la porte de nos foyers, c'est que le potentiel est énorme.

Il ne fait aucun doute que les produits du quotidien vont être de plus en plus connectés (comme nous avons pu le voir au CES cette année), mais pas toujours bien sécurisés. Les acteurs comme Google, Apple et Microsoft, qui ambitionnent qu'un maximum d'objets connectés puissent fonctionner à l'avenir avec leurs plateformes mobiles respectives, vont sans doute imposer aux fabricants un cahier des charges drastique en matière de sécurité s'ils veulent obtenir une certification. Cela pourrait peut-être permettre d'augmenter le niveau de protection des objets connectés, même si comme nous l'avons vu, il n'est pas toujours possible de patcher des produits comprenant des composants provenant de différents fabricants.

Le nombre croissant d'objets connectés risque d'intéresser de plus en plus les cybercriminels pour entreprendre des diffusions de spams ou de logiciels malveillants à grande échelle, par exemple. Mais le plus effrayant serait qu'ils puissent prendre le contrôle total des maisons intelligentes, espionner leurs habitants à l'aide des caméras de surveillance, s'introduire ni vu ni connu dans le foyer en déverrouillant la porte à l'aide d'un smartphone, couper l'électricité ou le chauffage en plein hiver, ou encore, déclencher l'alarme au beau milieu de la nuit…

Pour que les maisons intelligentes tiennent vraiment toutes leurs promesses, il est indispensable qu'à l'avenir leur sécurité soit garantie. En attendant, côté utilisateur, il faudra être de plus en plus vigilant, se renseigner sur le système de protection des produits, faire systématiquement les mises à jour, ou encore instaurer un mot de passe fort pour l'accès à distance de tous les appareils connectés. Le prix à payer pour que le rêve de posséder une maison intelligente ne tourne pas au cauchemar.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : #http://www.clubic.com/antivirus-securite-informatique/article-723729-1-objets-connectes-representent-risque.html
Par Jérôme Cartegini