FABRICE MATTATIA (90) *président du comité d'agrément des hébergeurs de données de santé*

OBJETS CONNECTÉS : LES CONDITIONS DE LA CONFIANCE

Les promoteurs des objets connectés, souvent pressés par le temps, par leur *business plan* et par la hâte de conquérir le marché avant les concurrents, consacrent tous leurs efforts à développer les fonctionnalités pratiques ainsi que le plan marketing, et négligent souvent deux aspects indispensables à l'instauration d'une confiance de long terme : la sécurité technique et la conformité juridique. Ils prennent ainsi des risques majeurs et s'exposent à de graves revers en cas de problème, ce qui ne serait pas grave s'ils n'y exposaient pas aussi leurs clients.

Le premier des risques est celui de la sécurité. Un inventaire à la Prévert constitue peut-être le meilleur moyen de donner un aperçu des failles de sécurité que recèlent bon nombre d'objets connectés mal conçus, et le résultat n'est pas rassurant. En octobre 2015, lors d'une conférence de presse du Premier ministre consacrée à la cybersécurité, les experts de l'Agence nationale de la sécurité des systèmes de l'information (ANSSI) ont montré comment ils pouvaient facilement pirater une montre connectée. Ils ont ainsi pu prendre le contrôle de l'objet, accéder aux SMS de son propriétaire, déclencher à son insu le microphone ou l'appareil photo intégré, connaître sa localisation… La montre connectée étant devenue un outil potentiel d'espionnage, son port est désormais interdit dans le gouvernement britannique lors des réunions du Conseil des ministres – les téléphones mobiles en étaient d'ailleurs déjà bannis, pour les mêmes raisons. De même, les microphones destinés à la commande vocale, par exemple sur un téléviseur connecté, peuvent être détournés pour espionner les conversations.

« Des microphones destinés à la commande vocale des téléviseurs connectés peuvent être détournés pour espionner les conversations »

DES VOITURES PIRATÉES

Concernant les voitures connectées, des chercheurs en sécurité ont réussi ces derniers mois à pirater des modèles de marques aussi diverses que Tesla, Jeep ou Toyota, à en prendre le contrôle à distance, et à leur faire effectuer des manœuvres diverses (ouverture des portes, allumage des phares, déclenchement des freins ou de l'accélérateur…). Il n'est pas besoin d'insister sur les risques pour les occupants et pour leur environnement, si ces attaques avaient été menées par des individus malveillants, et non par des chercheurs…

© HURRICANEHANK / SHUTTERSTOCK, INC.

La prise de contrôle à distance d'une montre connectée est possible.

REPÈRES

Depuis plusieurs années, on annonce l'arrivée imminente de « l'Internet des objets » (IoT, *Internet of things*), également désigné sous l'appellation « objets connectés ». Le développement des applications sur smartphone ou sur bracelet destinées à nous ausculter en permanence pour garantir notre santé, le succès relatif des objets à la mode comme les montres connectées ou les lunettes-caméras, et la connexion au réseau d'objets jusqu'ici traditionnels comme le compteur électrique ou la voiture, nous font entrer, lentement mais sûrement, dans ce nouvel univers. À terme plusieurs milliards d'objets seront potentiellement connectés.

© PAVEL L PHOTO AND VIDEO / SHUTTERSTOCK, INC.

Le risque du piratage à distance d'une automobile est avéré.

Chrysler a ainsi été contraint de rappeler 1,4 million de véhicules afin de mettre à jour la sécurité de leur système informatique.

DES MENACES QUI S'ÉTENDENT DE PLUS EN PLUS

Les compteurs d'électricité dits « intelligents » ne sont pas mieux lotis. Des failles de sécurité ont été découvertes sur ceux utilisés en Espagne, au Royaume-Uni ou en Allemagne, permettant de modifier leurs paramètres de fonctionnement, voire de couper le courant à tout un pays. Des attaquants ont pu également pirater des objets de santé, comme des pacemakers ou des pompes à insuline, menaçant la santé des patients : c'est pour éviter des tentatives d'assassinat que le vice-président américain Dick Cheney avait désactivé la connexion de son pacemaker. Les failles de sécurité qui permettent ces piratages sont de toutes sortes. Un défaut de chiffrement et de signature des mises à jour, permettant à l'attaquant de modifier la programmation de l'objet en se faisant passer pour le constructeur, a ainsi été constaté sur des thermostats de chaudière ou sur des télévisions connectées, permettant potentiellement une prise de contrôle hostile menant à un sabotage ou à une demande de rançon. Quand l'accès à l'objet est protégé par un mot de passe (par exemple sur une box Wi-Fi), il n'est pas rare que ce soit le mot de passe par défaut qui soit systématiquement utilisé, et il arrive même, comble de mauvaise conception, qu'un défaut de programmation empêche de changer ledit mot de passe ! Les données collectées par l'objet (par exemple un capteur de pouls ou de pression dans un bracelet) peuvent être stockées et/ou transmises sans être chiffrées, devenant ainsi lisibles par n'importe qui.

« Il arrive qu'un défaut de programmation empêche de changer un mot de passe »

PEARL HARBOR NUMÉRIQUE

On constate ainsi, malheureusement, que la sécurité informatique n'est pas assez prise en considération lors de la conception des objets connectés qui envahissent notre quotidien. Dans ces conditions, on peut craindre une attaque étatique ou terroriste visant à s'emparer d'un seul coup du contrôle de toute une catégorie d'objets stratégiques au niveau national, par exemple pour couper le courant définitivement dans tout un pays – ce qui constituerait un véritable Pearl Harbor numérique.

DES RISQUES JURIDIQUES MAL CONNUS ET SOUS-ESTIMÉS

En comparaison, les risques de non-conformité juridique représentent des enjeux bien moins vitaux. Pourtant, ils témoignent eux aussi d'une négligence lors de la conception des objets connectés et des services qu'ils alimentent, et sont donc un symptôme du manque de sérieux de l'entreprise – ou d'une désinvolture envers les lois, ce qui n'est pas bon signe non plus. En manipulant, en transmettant et en stockant des données relatives aux habitudes de leur propriétaire, les objets connectés relèvent des lois sur la protection des données personnelles. Si les données traitées sont considérées comme sensibles (données médicales notamment), la loi impose des précautions supplémentaires. Et pour les données de santé elles-mêmes, le code de la santé prévoit un régime particulier pour le stockage.

DES CAMÉRAS INFECTÉES PAR UN VIRUS

En septembre 2016, l'hébergeur OVH a été la cible de la plus importante attaque en saturation (DDOS, *distributed denial of service*) jamais enregistrée, menée à partir… d'un réseau de 150 000 caméras de surveillance infectées et contrôlées à distance par un pirate informatique qui a utilisé un *malware*.


© ASCAIN64 / FOTOLIA.COM

La société OVH a été victime d'un piratage *via* des caméras de télésurveillance.

MÉCONNAISSANCE DE LA LÉGISLATION

Or, les industriels qui diffusent les objets connectés ignorent le plus souvent leurs obligations légales, surtout lorsqu'il s'agit de PME ou de *start-up*. EDF, en revanche, a pris soin de consulter la Commission nationale de l'informatique et des libertés (CNIL) au sujet de son compteur Linky. Obligation d'information des clients, de sécurisation des données, limitation de la durée de conservation, interdiction de stocker les données hors de l'Union européenne sauf dérogations… Le recours à un juriste est indispensable pour s'y retrouver.

« Consulter des spécialistes de la sécurité informatique et du droit pour valider les choix fonctionnels et les choix d'implémentation »

L'IMAGE DE MARQUE EN PREMIÈRE LIGNE

Le risque pour l'entreprise en cas de non-conformité réside d'abord dans l'atteinte à son image de marque, car les consommateurs exigent désormais que leurs données soient protégées. Or l'image de marque représente un actif considérable. Yahoo, qui vient de perdre les données de 500 millions de clients, le paye immédiatement en perte de valeur boursière (Verizon, qui était sur le point de racheter Yahoo, exige une renégociation à la baisse de la transaction pour un milliard de dollars). Existent également les sanctions pénales et administratives : cinq ans de prison et 300 000 euros d'amende au pénal, et jusqu'à 3 millions d'euros d'amende devant la CNIL (à partir de 2018, ce sera 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise). Les consommateurs sont de plus en plus sensibles à la protection de leurs données, et en conséquence, les sanctions prononcées en cas de violation des obligations ont tendance à s'alourdir.

INTÉGRER LES RISQUES DÈS LA PHASE DE CONCEPTION…

De manière générale, il est primordial de ne plus négliger les risques de sécurité et les risques juridiques, et de les placer au contraire au centre de la démarche de conception des services connectés. Ainsi, dès le début de la conception, au niveau des spécifications, il convient de consulter des spécialistes de la sécurité informatique et du droit, pour valider les choix fonctionnels et les choix d'implémentation.

… ET PENDANT TOUTE LA VIE DU PRODUIT OU SERVICE

Une analyse de risques devra être systématiquement menée : sachant qu'aucune protection n'est inviolable (même la NSA s'est fait pirater ses données confidentielles…), que risque le client le jour où un attaquant réussira à accéder au système ? S'il y a risque d'atteinte grave à la sécurité des personnes, c'est toute la pertinence de la démarche qui doit être remise en question. Des assurances peuvent également être utiles. Des mécanismes spécifiques d'atténuation du risque et de protection des données et des systèmes se révèlent indispensables. En outre, il ne suffit pas d'installer ces protections lors de la vente du produit : un suivi continu est indispensable, ainsi que des mises à jour par un canal sécurisé.

DES MESURES À LA HAUTEUR DES ENJEUX

La conformité juridique et la sécurité informatique doivent ainsi représenter une préoccupation constante des concepteurs et des fournisseurs de systèmes connectés. Les mesures de protection doivent être à la mesure des risques : si on fait courir au pays un risque d'importance vitale (par exemple, la moindre possibilité d'une prise de contrôle hostile de toute la distribution d'électricité, ou de tous les véhicules, au niveau national), les mesures de sécurité doivent être adaptées. Cela représente un surcoût financier, qui diminuera certes l'attrait des objets connectés. Mais ce surcoût est indispensable à notre liberté et à notre indépendance futures. ■

© TRIFF / SHUTTERSTOCK, INC.

Même la NSA s'est fait pirater des données confidentielles.

BIBLIOGRAPHIE (SÉLECTION)

Le droit des données personnelles, 2e édition, Eyrolles, 2016.
Internet et les réseaux sociaux : que dit la loi ? 2e édition, Eyrolles, 2015.
Le droit des données personnelles : n'attendez pas que la CNIL ou les pirates vous tombent dessus, Eyrolles, 2016.
Être propriétaire de ses données personnelles ? avec Morgane Yaïche, revue *Lamy Droit de l'immatériel*, avril et juin 2015.
« De l'utilité d'une carte d'identité électronique pour sécuriser le monde numérique », *Annales des Télécommunications*, 62, n° 11-12, 2007.
« Panorama de l'informatisation du secteur de la santé », *La Jaune et la Rouge*, février 2003.
« La sécurisation des échanges électroniques », *La Jaune et la Rouge*, décembre 1999.