99

CIO.FOCUS

Juin 2015

La sécurité des données personnelles à l'heure des objets connectés

En bref

Les objets connectés envahissent de plus en plus notre quotidien. La montre ou le gadget de surveillance pseudo-médicale sont certes les objets auxquels on pense spontanément. Mais il ne faut pas oublier d'autres objets, de l'automobile au compteur d'énergie communiquant, aux enjeux bien plus importants et concernant une population bien plus vaste.
Ces objets peuvent être l'objet de piratage autant pour voler des données personnelles que pour provoquer un dysfonctionnement. Leur sécurité est un enjeu majeur pour les RSSI. Pas demain. Aujourd'hui.

Sommaire

Juridique

Le contexte concurrentiel atténue le paradoxe entre objets connectés et sécurité

Olivia Luzi, Avocat associé cabinet Féral-Schuhl / Sainte-Marie. Photo : Bruno Lévy.

Le 19 mai 2015, CIO a organisé une matinée stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI ». Olivia Luzi, Avocat associé cabinet Féral-Schuhl / Sainte-Marie, y a apporté son expertise.

« Le sujet des objets connectés ne concerne pas encore tout le monde mais devrait toucher un nombre beaucoup plus important de personnes dans les années à venir ». Sans pour autant jouer la Cassandre, Olivia Luzi, Avocat associé du cabinet Féral-Schul / Sainte-Marie, a directement posé le débat en montant sur la scène de l'événement CIO Sécurité qui se déroulait le 19 mai 2015. Elle le rappelle, les statistiques font état de 15 milliards d'objets connectés aujourd'hui mais estime que leur nombre passera à 80 milliards d'ici 2020.

« Si leur intervention est, pour l'instant, peu présente dans le monde de l'entreprise, la logique de l'internet des objets se répand de manière très conviviale à travers les smartphones, les bracelets ou encore les montres qui vont collecter de nombreuses données sur votre environnement. Nous l'avons vu, certains comme Direct Assurance commencent à se baser sur ces données pour proposer des contrats automobiles personnalisés en fonction des kilomètres parcourus et de la conduite », résume la juriste. Elle ajoute que toutes ces données, une fois assemblées, permettent de résumer l'activité des personnes utilisant les objets, et de la partager avec une forte dimension sociale.

Des avantages commerciaux sont également mis en avant comme dans les centres commerciaux qui peuvent vous envoyer des notifications en fonction de votre position dans le magasin. « Derrières ces aspects pratiques et conviviaux, nous avons

malheureusement tendance à oblitérer les risques induis par l'utilisation des objets connectés qui échangent en permanence des informations sur les réseaux », constate toutefois Olivia Luzi.
Pour elle, les risques principaux portent sur les failles de sécurité et le détournement des données. « Si ces données touchent à votre santé, les risques sont multipliés, quelques soient les personnes qui les récupèrent, aussi bien des assureurs que des pirates », enchérit l'avocate. La perte pure et simple du contrôle des données est aussi à surveiller. « Quand vous acceptez de partager un certain nombre d'informations sur les réseaux sociaux, différentes instances peuvent facilement se livrer à du profilage en les recoupant », précise Olivia Luzi.
Elle appuie également sur la prépondérance des compagnies d'assurances dans ce domaine. Elle raconte : « Axa, en partenariat avec WeThings, a organisé un concours afin d'offrir aux souscripteurs d'une certaine offre des bracelets connectés pour réaliser certains challenges. Or les conditions générales du concours prévoient que WeThings sera le seul propriétaire des données qui seront détruites dès la fin de l'événement ». Sauf qu'en creusant un peu, il s'avère que les utilisateurs doivent réclamer leurs lots directement auprès d'Axa et que par ce biais, l'assureur va identifier certaines informations sur les assurés. « Ce transfert d'informations n'est pas clairement stipulé dans les conditions du règlement. Je ne dis pas qu'Axa va utiliser ces données pour faire du profilage mais la compagnie aurait pu être plus transparente », tranche Olivia Luzi.

Les entreprises encore peu concernées

La question qui se pose aujourd'hui reste que les données personnelles ne sont pas encore au coeur des préoccupations des entreprises. « Ces dernières viennent souvent nous voir pour des audits CNIL afin de vérifier que les traitements et la sécurité des données sont en conformité avec la Loi Informatique et Libertés », explique la juriste. Pour elle la question est donc de voir si le cadre juridique apporte des garanties suffisantes et s'il y a des axes d'amélioration possibles pour l'avenir.
Pour commencer elle note que la Loi Informatique et Libertés ne s'applique pas dans tous les cas. « Logiquement, les responsables de traitement des données, qu'ils soient basés en France ou à l'étranger doivent être soumis à cette loi. Mais dans les faits, quand ils sont installés dans des pays exotiques, vous avez le plus grand mal à la faire appliquer », explique Olivia Luzy. Elle revient également sur la transparence imposée par la Loi Informatique et Libertés. « Personnes ne peut récolter vos données à votre insu et il faut qu'elles soient pertinentes avec la finalité du traitement. La durée de conservation des informations doit également être en accord avec cette finalité », précise la juriste.

Sur l'aspect sécurité informatique, la Loi Informatique et Libertés prévoit également un certain nombre de dispositions à charge des responsables de traitement et des sous-traitants. « Les moyens mis en oeuvre doivent être proportionnels à la criticité des données pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès », détaille Olivia Luzi.
Elle revient sur l'incident qui avait touché Orange à l'été 2014. « La CNIL avait alerté sur le fait que même si la faille ayant entraîné la fuite était le fait du sous-traitant, le responsable de traitement aurait dû mener un audit de sécurité pour éviter l'incident », rappelle-t-elle.
En plus de la CNIL il va falloir en outre composer avec le règlement européen qui devrait être mis en place d'ici la fin de l'année 2015. Les données de santé sont également visées par la dernière Loi Santé qui exige des certifications strictes pour leur

traitement et leur hébergement. L'avocate revient également sur la question du CIL. « Il a un intérêt pour être dispenser des déclarations de traitements mais il est toutefois tenue de remplir des autorisations et d'obtenir un accord de la CNIL avant que ne soit lancée l'opération », rappelle Olivia Luzi.

Jusqu'à 100 M€ d'amende

Les sanctions de cette autorité administrative indépendante ne sont pas non plus à négliger. Les amendes peuvent aller jusqu'à 300 000 euros pour une personne physique et 1,5 million d'euros pour une personne morale. En outre, des sanctions pécuniaires de 150 000 euros peuvent être prises en cas de certains manquements. « Cette somme n'est pas forcément très dissuasive mais ces sanctions vont être considérablement renforcées avec l'arrivée du règlement européen et devraient devenir beaucoup plus dissuasives », met en garde la juriste. Elles pourraient être calculées en fonction du chiffre d'affaires et s'élever jusqu'à 100 millions d'euros.

« Dans les axes d'améliorations que nous pouvons identifier, il y a notamment la sensibilisation des personnes », enchaîne Olivia Luzi. C'est un fait, les gens ont tendance à partager de nombreuses informations sans se douter de l'utilisation qui peut en être faite. « Il va également falloir compter avec la démocratisation du *privacy by design* qui permet justement de limiter les risques dès la création des applications et le *privacy by default* qui assure un paramétrage de la sécurité à un niveau maximal, contrairement à ce qui se fait actuellement », poursuit la juriste.
Olivia Luzi évoque également la mise en place de normes et de labels pour indiquer aux consommateurs quelles sont les applications les plus respectueuses de la vie privée et de la protection des données personnelles. « A mon sens, il n'y a pas de paradoxe entre l'essor des objets connectés et le souhait de protéger ses données personnel. Dans un monde très concurrentiel, les applications et les objets qui vont être utilisés par le plus grand nombre devront respecter ces objectifs et montrer au grand public qu'ils sont respectueux de leur vie privée », conclut Olivia Luzi.

EN SAVOIR PLUS:

Télécharger les présentations de la conférence (Cet espace s'enrichit au fur et à mesure de la disponibilité des éléments)

Oscar Barthe
Journaliste

Stratégie

Objets connectés : tout doit commencer par une bonne étude de risques

Philippe Loudenot et le Commandant Michel Dubois, membres du CESIN (de droite à gauche) - Photo : Bruno Lévy.

Le 19 mai 2015, CIO a organisé une matinée stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI ». Philippe Loudenot et le Commandant Michel Dubois, membres du CESIN, y ont apporté leur expertise.

Conviés à une table ronde de l'événement, « Sécurité : données personnelles aux objets connectés » du 19 mai 2015 , Philippe Loudenot, fonctionnaire de sécurité des SI aux Ministères chargés des affaires sociales, et le commandant Michel Dubois, officier de sécurité des SI au Service de Santé des Armées, sont venus apporter leur pierre à l'édifice. Tous deux membres du CESIN (Club des Experts de la Sécurité Informatique et du Numérique), ils sont largement mobilisés par ces problématiques. Philippe Loudenot gère ainsi les SI de trois ministères différents (Sport, Travail et Santé) qui sont, selon lui, parmi les plus concernés par les objets connectés aujourd'hui. Tous les deux sont en outre confrontés au cas bien particulier des données de santé.

Pour entamer la table ronde, ils ont d'ailleurs pointé une défaillance sur la phase par laquelle tout le monde devrait commencer. « Objet connectés ou non, malheureusement, aucune étude de risques n'est jamais réalisée, quelle que soit le type de SI. C'est catastrophique », débute Philippe Loudenot. Il trouve même surprenant les résultats de l'étude CIO, présentés en début d'événement, qui disent qu'un quart des entreprises réalisent ou souhaitent réaliser une étude de risques sur les objets connectés. « Les gens ne savent pas ce qu'ils veulent protéger, contre qui et contre quoi », lance le fonctionnaire de sécurité.
De son côté, Michel Dubois abonde dans ce sens mais sait très bien contre quoi il doit

se protéger. « Nous faisons bien évidemment l'analyse des risques sur nos équipements et nos SI avant d'envoyer nos militaires sur le terrain. Mais certains partaient avec leur montre connectée et nous nous sommes rendud compte qu'il était tout à fait possible de tracer leurs déplacements sur le terrain d'opérations », explique le commandant. Des campagnes de sensibilisation sont ainsi menées pour mettre une terme à ces aberrations. Il reconnaît, en outre, qu'il y a sûrement déjà eu des cas de piratages de données GPS émises par les objets connectés des soldats de l'armée française.

Nous sommes concernés à tous les niveaux

Mais si pour les objets grand public qui n'ont pas de rapport avec l'entreprise, il est possible d'interdire leur usage, c'est bien sûr très différent avec ceux qui contribuent à son bon fonctionnement. « Il est vrai que nous pensons tous à la petite montre, mais il y a aussi des tonnes d'objets connectés, notamment dans les environnements biomédicaux. Récemment nous nous sommes rendus compte qu'il était possible de pirater les pousse-seringues qui gèrent les doses de produits administrés aux patients. Si vous injectez 300ml au lieu de 3ml de morphine à un malade, il meurt », raconte Michel Dubois.
En outre, les très gros équipements comme les télé-scanners et les IRM sont des appareils qui sont infogérés par leur fabricant. « Difficile de savoir exactement où vont les données. Or nous sommes tenus d'avoir recourt à ces contrats de télémaintenance sans quoi le fonctionnement de l'appareil n'est pas assuré », déclare le militaire. En 2009, un appareil qui n'était pas protégé a ainsi permis une intrusion dans un système hospitalier. Selon lui, ces lacunes sont en train d'être comblées mais un grand travail de fond doit être fait.

« Dans le civil, la problématique est exactement la même », reconnaît Philippe Loudenot. Les produits de santé, que ce soit dans l'armée ou ailleurs, sont confrontés aux mêmes problématiques. « J'ai tout à l'heure entendu le termes de *privacy by design* qui m'a beaucoup plu et qu'il ne faut pas hésiter à élargir au *security by design*. Il faut prendre le problème directement à sa source », lance le fonctionnaire de sécurité. Il prend notamment l'exemple des pacemakers et des défibrillateurs dont il a été prouvé récemment qu'il était possible d'en prendre le contrôle à distance. « Dick Chenney, l'ancien vice-président des États-Unis, est repassé sur latable d'opération pour se faire désactiver tous les systèmes de paramétrage et de contrôle à distance de son pacemaker », rappelle Philippe Loudenot.
Il revient à l'analyse des risques et prend l'exemple des balances connectées qui fonctionnent par bio-impédance. « Elle peuvent détruire les pacemakers. Nous sommes dans un cas ou un objet connecté peut en annihiler un autre dans son fonctionnement normal. C'est typiquement le genre de risques que nous devons pouvoir prendre en compte », explique le fonctionnaire de sécurité. Au regard des statistiques, il estime que nous courrons un grave danger.

"Ne pas non plus tirer sur l'ambulance"

L'affaire du pirate ayant réussi ces derniers mois à s'introduire dans les systèmes d'un avion de ligne en plein vol n'est pas là pour lui donner tort. « Attention tout de même, il faut se méfier des journalistes [sic] », tempère Michel Dubois. Il suit la situation depuis quelques temps et assure qu'il ne sert à rien de tirer sur l'ambulance. « Cela fait plusieurs fois que ce garçon réalise de telles opérations et tente d'alerter les constructeurs, en vain », rappelle le commandant.

Il pointe du doigt la très mauvaise gestion de la situation de la part du FBI qui a décidé de le mettre en prison malgré sa volonté d'alerter : « Typiquement, c'est de la mauvaise gestion des risques. Au lieux de corriger l'erreur, ils punissent celui qui alerte. Il n'a fait que mettre en évidence des vulnérabilités ». Selon lui, la plupart des objets connectés, et notamment les véhicules, sont vulnérables. « Nous avons un métier d'avenir », constate-t-il avec ironie. De son côté, Philippe Laudenot prend l'exemple cocasse de toilettes japonaises (avec des jets d'eau pour nettoyer leurs usagers) piratées ayant copieusement arrosé leurs utilisateurs.

Au delà de l'objet lui même, la préservation des donnés pose également problème. « Il y a régulièrement des études pour vérifier l'usage des données », rassure Philippe Laudenot. Selon lui la recherche d'informations est toutefois devenu un sport éminemment pratiqué par les entreprises, notamment concernant des données de santé. Il suffit de regarder les sommes mises sur la table par Amazon et Goggle sur le sujet pour s'en rendre compte. « Le dossier médical partagé que la France tente d'instaurer depuis un petit bout de temps, a déjà été mis en place depuis plus de 10 ans par Google, et il fonctionne très bien », enchérit Michel Dubois. En outre, il rappelle que lorsque vous faite une recherche sur le moteur de recherche de la firme de Mountain View, vous lui donnez une information.

Toujours la sensibilisation

« En outre, aujourd'hui, les gens achètent des objets sans lire les conditions d'utilisation ni les précautions d'emploi et beaucoup d'informations partent dans la nature », lance Philippe Laudenot. Grossissant le trait, il en vient même à mettre en doute l'utilité de la CNIL. « Elle a été créé en 1978 suite au projet Safari qui visait à ficher les citoyens. Si aujourd'hui je suis une force de police, je n'ai qu'à me rendre sur les réseaux sociaux pour trouver des fichiers qui sont à jour », explique Philippe Laudenot.
Il fait alors remarquer que sur les sites médicaux, c'est exactement la même chose. Les gens révèlent leurs symptômes, leurs traitements, etc. « Nous sommes dans une situation paradoxale ou le citoyen donne ses données de bon coeur sans savoir ce qui en sera fait », résume-t-il. Michel Dubois dénonce ainsi le manque de prise de conscience. « Dans un hôpital, certains employés ont pris l'initiative de créer un formulaire en ligne pour les patients avec la date de naissance et les symptômes. La page web n'est pas chiffré rien n'est protégé », illustre-t-il.

En savoir plus

Télécharger les présentations de la conférence (Cet espace s'enrichit au fur et à mesure de la disponibilité des éléments)

Oscar Barthe
Journaliste

Technologies

Dès aujourd'hui, la sécurisation des objets connectés n'est plus une option

Nacira Salvan (Safran) et Sylvain Géron (Polyconseil Autolib BlueSolutions) – de droite à gauche, photo : Bruno Lévy

Le 19 mai 2015, CIO a organisé une matinée stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI ». Nacira Salvan (Safran) et Sylvain Géron (Polyconseil Autolib BlueSolutions) y ont témoigné.

Les objets connectés, au sens large, ont déjà envahi notre quotidien tant personnel que professionnel. Et la sécurité n'est plus du tout une option tant les données qui sont créées ou émises par ces objets sont parfois sensibles. Lors de la matinée stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI » organisée à Paris par CIO, Nacira Salvan, responsable architecture sécurité de Safran, et Sylvain Géron, directeur associé de Polyconseil Autolib BlueSolutions (groupe Bolloré), ont apporté leur témoignage sur leurs bonnes pratiques en la matière.
D'origine française et opérant dans des secteurs très sensibles (défense, aéronautique...), le groupe Safran dispose de 280 sites dans le monde pour un effectif global de 70 000 collaborateurs dont 18 000 aux Etats-Unis et 3500 en Chine. Tant les secteurs que certains pays d'implantation sont en eux-mêmes des facteurs de risques sur la sécurité des systèmes d'information. Safran gère bien entendu des terminaux mobiles classiques (smartphones...), de l'électronique embarqué dans des véhicules (notamment des avions) et a travaillé avec Valéo au guidage des voitures sans GPS d'après une captation de l'environnement. Le GPS est en effet une fragilité en lui-même : soumis au bon vouloir d'un gouvernement étranger et susceptible d'être brouillé par des pirates souhaitant détourner le véhicule guidé (y compris des drones militaires).

De son côté, le service Autolib, mis en place à Paris par le Groupe Bolloré est par nature basé sur des objets connectés, en l'occurrence les automobiles Bluecar. Autolib propose un service de véhicules électriques partagés que chaque utilisateur peut louer à la demande le temps d'un trajet urbain en région parisienne. La facturation repose sur l'usage réel et la bonne marche du service implique donc de suivre la position de chaque véhicule ainsi que son utilisation par quel conducteur.

Sécuriser le BYOD

Mais les premiers objets connectés, dans une entreprise, sont en général plus simples qu'un véhicule inséré dans un service complexe. Il s'agit simplement des multiples terminaux mobiles connectés. Et quand le terminal en question est le joujou d'un directeur métier, il est impossible de le refuser. « La problématique du BYOD arrive en général par le top management » reconnaît Nacira Salvan. Safran a cependant rejeté le concept de BYOD au profit de celui de COPE.
La DSI doit cependant déjà être bien contente si elle sait qu'un iPhone se connecte au système d'information. Nacira Salvan souligne : « il est impossible de demander à un top manager de s'identifier quatre fois pour connecter son terminal personnel au système d'information en sécurisant sa connexion. » Or plus le niveau hiérarchique de l'utilisateur s'accroît, plus le niveau de sensibilité potentielle des données échangées sur son terminal, notamment par mail, s'accroît également.
« Un tel utilisateur va de toutes façons chercher à se connecter au système d'information comme il l'entend, autant faire l'analyse de risque et prendre les mesures adéquates en amont » insiste Nacira Salvan. Cela passe par l'authentification forte. Mais tous les moyens de sécurité, pour être mis en oeuvre, supposent une adhésion des utilisateurs faute de quoi ceux-ci chercheront un moyen de les contourner. Nacira Salvan reconnaît : « la conduite du changement est nécessaire mais on ne peut pas non plus demander à des top managers de recopier un mot de passe à usage unique donné par une application pour se connecter à un VPN avant de s'authentifier une deuxième fois pour accéder à tel système, etc. » L'accès doit être simple et sécurisé. Safran a donc choisi des solutions du marché qui sécurisent le poste de manière simple. Safran sait donc à chaque connexion quel terminal se connecte, avec quel utilisateur et dans quel contexte (dans ou hors des murs de l'entreprise par exemple). Et les droits du terminal (y compris la connexion Internet) seront strictement limités en fonction de ce contexte. Dans certains pays, le contexte implique, même dans les murs de Safran, des mesures particulières et le blocage de certains droits d'accès au système central.
Techniquement, le BYOD ou les terminaux mobiles d'entreprises peuvent être suffisamment sécurisés. « Mais sur le BYOD, la question est juridique : un outil de sécurité de l'entreprise pourrait-il détruire des données personnelles de l'utilisateur ? » soulève Nacira Salvan.

Sécuriser les données associées aux véhicules connectés

Les droits d'accès et la sécurité doivent être particulièrement bien gérés lorsqu'il s'agit d'un véhicule automobile. En effet, cet objet connecté a comme particularité de pouvoir révéler tous les déplacements opérés grâce à lui, donc potentiellement tous les déplacements de ses chauffeurs successifs. « Pour Autolib, la question de la sécurité a été traitée dès le départ » rassure Sylvain Géron.
Polyconseil a reçu la mission de concevoir le système d'information d'Autolib à Paris en février 2011 pour une ouverture commerciale en décembre de la même année. Même si la sécurité n'est pas la première pensée que l'on a quand on doit mener un tel projet

en dix mois, l'architecture a été conçue pour être sécurisée dès le départ. Sylvain Géron se souvient : « nous avons notamment rapidement pris contact avec la CNIL pour savoir comment nous devions traiter les données personnelles. Celles-ci ont ainsi été totalement séparées des données de trajet dans l'architecture même du système d'information. » Et la sécurité même du véhicule a fait l'objet d'une grande attention. Ainsi, aucun dispositif ne peut commander à distance le véhicule, y compris pour le stopper ou, au contraire, désactiver les freins. « C'est physiquement impossible » martèle Sylvain Géron.
Mais il existe aussi des risques plus classiques qui prennent une dimension particulière dans ce genre de projets. « Lors du lancement, un constructeur automobile allemand a tenté de pénétrer le système, ce qui nous a amené à réfléchir de nouveau à la manière de renforcer la sécurité » rappelle Sylvain Géron. Un RSSI permanent a été embauché. L'analyse des risques a été reprise en totalité. Un audit complet a été mis en oeuvre avec, notamment des tests d'intrusion. « Même s'il y a quelques petites choses à corriger, l'audit s'est plutôt bien passé et a conclu que nous avions bien travaillé » indique Sylvain Géron.

Séparer les données pour les sécuriser

Mais nul ne peut se prévaloir d'être toujours à l'abri. Pour éviter qu'un éventuel piratage n'ait rapidement des conséquences trop importantes, les bases de données avec les informations sur les clients et celles avec les informations sur les véhicules et leurs déplacements sont totalement séparées. Rapprocher les données -pour la facturation par exemple- suppose de faire partie du très petit nombre de personnes qui ont une vraie raison pour cela. Sylvain Géron insiste : « même pour répondre à une sollicitation de la police, il est physiquement impossible de suivre en temps réel une personne, le suivi ne pourra qu'être *a posteriori*. »
Assez curieusement, aucun client n'a jamais posé de questions sur la sécurité d'Autolib. « Mais si nous avions eu un incident grave, parions que cela serait devenu un sujet pour nos clients » reconnaît Sylvain Géron. Nacira Salvan soupire : « il faut qu'il y ait un gros problème pour que l'on prenne conscience des risques, dans tous les domaines, y compris pour les objets grand public comme les montres connectées. Acceptera-t-on demain d'avoir un capteur de glycémie qui incitera son assureur à augmenter le montant de sa police d'assurance en cas de diabète ? »

Les anciens systèmes connectés sans précautions

Si Autolib -système récent- a été conçu dès l'origine comme très sécurisé, ce n'est pas le cas de systèmes plus anciens. Nacira Salvan a notamment travaillé sur les systèmes industriels (de type SCADA) qui ont été conçus initialement pour être totalement séparés du réseau général de l'entreprise et d'Internet. Elle a ainsi traité une analyse de risques de systèmes industriels en milieu très contraint dans l'industrie nucléaire. « En tel cas, une analyse de type Ebios, avec probabilité et impact, n'a pas de sens : même un risque très improbable doit être traité car sa réalisation déclencherait une catastrophe majeure, éventuellement de type Tchernobyl » explique Nacira Salvan. En l'occurrence, il s'agissait de permettre une supervision de capteurs physiques, la transmission des données s'opérant à travers le réseau informatique de l'établissement.
Nacira Salvan pointe : « la prise de conscience des risques encourus par les systèmes Scada date de l'affaire Stuxnet où un malware a détruit des systèmes industriels iraniens à partir de la contamination par une clé USB. » Conçus pour ne pas être connectés, les systèmes Scada sont souvent vulnérables à pratiquement tous les niveaux, même sur des basiques comme le mot de passe. « Vous pouvez déclencher

de nombreuses morts en modifiant la quantité de chlore injectée dans l'eau courante d'une ville, vous pouvez faire exploser une centrale nucléaire en piratant les capteurs de température » s'alarme Nacira Salvan.

La sécurité concerne bien sûr les données sortantes des objets connectés, celles qui vont être utilisées pour le pilotage d'une usine ou d'un installation de type industrielle. Récupérer de telles données peut avoir du sens : connaître le rythme d'une chaîne de montage, par exemple, peut donner beaucoup d'informations sur l'activité d'une entreprise. Sylvain Géron observe : « la première faille est toujours humaine, comme nous l'a rappelé l'affaire Snowden où des données très sensibles ont été sorties manuellement. » Face à ces risques, tous les salariés d'Autolib reçoivent régulièrement des rappels de sécurité.

Mais on peut aussi imaginer un piratage crapuleux visant à altérer des données entrantes, par exemple pour déclencher une autodestruction d'une coûteuse chaîne de production lors d'un chantage avec extorsion de fonds. Est-ce vraiment de la science-fiction ? « Chez nous, la menace ne serait pas pertinente car notre architecture interdit un danger trop important pour les véhicules, même si nous avons eu des tentatives d'intrusion » explique Sylvain Géron. Mais la question reste ouverte concernant des systèmes Scada...

Bertrand Lemaire
Rédacteur en chef de CIO

Business

Le compteur communiquant, l'objet connecté pour tous à sécuriser

Yann Padova, commissaire à la Commission de Régulation de l'Energie - Photo : Bruno Lévy.

Le 19 mai 2015, CIO a organisé une matinée stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI ». Yann Padova, commissaire à la Commission de Régulation de l'Energie et ancien secrétaire général de la CNIL y a témoigné sur les compteurs intelligents.

Les objets connectés commencent à envahir notre quotidien mais il en est un auquel nul n'échappera : le compteur communiquant. Toute personne disposant d'un abonnement à un fournisseur d'électricité devra en effet en être doté dans les prochaines années, livrant potentiellement d'importantes quantités d'informations sur l'usage des appareils électro-domestiques voire l'occupation d'un logement. 35 millions d'unités vont être déployés chez les particuliers de cette année à 2021, pour un coût global de six milliards d'euros financés par la taxe d'accès au réseau sous la responsabilité du réseau ERDF, les entreprises étant déjà équipées dans la plupart des cas d'un compteur avec télérelève différent. Et cet objet est donc le parfait exemple pour s'interroger sur la sécurité des objets connectés et sur celle des données personnelles qu'ils peuvent traiter.

Ancien secrétaire général de la CNIL, Yann Padova est aujourd'hui commissaire à la Commission de Régulation de l'Energie (CRE). Il est intervenu à la Matinée Stratégique « Sécurité : des données personnelles aux objets connectés, les nouveaux défis des RSSI » organisée le 19 mai 2015 à Paris par CIO. Le compteur communiquant, les données personnelles traitées et leur sécurité sont évidemment au coeur de ses préoccupations.

Réguler le marché pour garantir la libre concurrence

La Commission de Régulation de l'Energie (CRE) est une autorité administrative indépendante, comme la CNIL ou le CSA, régulateur du secteur de l'énergie. Elle se préoccupe d'une part de l'accès au marché par les fournisseurs d'énergie et, d'autre part, du réseau de distribution. Son rôle va donc consister à surveiller les tarifs de gros, ceux de l'accès au réseau, etc. « Nous veillons ainsi à ce qu'il y ait libre concurrence et donc libre accès des fournisseurs d'énergie au réseau desservant les consommateurs » explique Yann Padova. Six commissaires, dont Yann Padova, et 130 collaborateurs opèrent sur ces missions.
La récente arrivée de Yann Padova à la CRE est liée à sa nomination par la président de l'Assemblée Nationale. Or la Loi prévoit que le commissaire à nommer devait être compétent en matière de données personnelles, ce qui était bien sûr le cas de l'ancien Administrateur de l'Assemblée Nationale et ancien Secrétaire Général de la CNIL Yann Padova. « Que la Loi prévoit cela n'est évidemment pas un hasard : le développement des smart-grids, des réseaux intelligents et des compteurs communicants est associé à de gros enjeux en matière de données personnelles et de sécurité de celles-ci » relève Yann Padova.

Un projet plus vaste que le seul compteur communiquant

Le compteur communiquant n'est pas un projet « tombé du ciel ». Il s'inscrit dans un vaste plan européen baptisé « 3 fois 20 » défini en 2008 sous présidence française : 20% de réduction de la consommation d'énergie, 20% de réduction des émissions de gaz à effet de serre, 20% de production d'énergie avec des moyens renouvelables. Yann Padova explique que « pour atteindre ces objectifs, cela suppose une vraie révolution des réseaux d'énergie autour de trois thèmes.
Le premier thème est celui de la production d'énergie. Les usines centralisées, à base de charbon ou de nucléaire, laissent la place à de plus petites unités. Le cas échéant, les consommateurs peuvent être aussi producteurs, par exemple en installant des panneaux solaires sur leur toit, voire de stockage via les batteries, notamment celles des voitures électriques.
Le deuxième thème est celui des nouveaux usages avec de forts impacts sur la production et la consommation d'électricité. Yann Padova prend l'exemple de l'automobile électrique qui « augmentera ponctuellement la consommation en pointe de 11% à parfois jusqu'à 100% localement dans certains endroits si l'on ne change pas nos modes de consommation. On en peut donc pas arriver à deux millions de véhicules électriques sans changer le réseau et les comportements ».
Ces changements impliquent un défi, le troisième thème, celui de l'information. « Le consommateur doit devenir consom' acteur, sensible à ses sources de consommation et à l'optimisation de sa consommation » juge Yann Padova. C'est le rôle du compteur communiquant Linky. Le commissaire insiste : « c'est la brique qui apporte l'intelligence au réseau ».

L'information consommateur au coeur du dispositif Linky

Linky est capable d'échanger de l'information dans les deux sens : de l'information entrante d'un côté, de l'information sortante de l'autre. Le compteur fait ainsi partie du dispositif visant à la maîtrise de la consommation. Les informations détaillées sur la consommation devront ainsi être publiées par le distributeur sur un site web, quasiment en temps réel. C'est aussi un dispositif qui vise à accroître la concurrence. En effet, comme le pointe Yann Padova, « le but est que des fournisseurs puisse proposer de l'énergie à des tarifs agressifs construits selon votre profil. » Les consommateurs

pourront donc choisir de donner accès à leurs donnés à certains fournisseurs afin que ceux-ci puissent étudier leur profil et faire une offre adaptée.
Enfin, Linky sera aussi un facteur d'innovation. Les données, à la fois techniques et personnelles, pourront être agrégées et servir à construire des services innovants par des nouveaux acteurs. Yann Padova envisage ainsi : « des conseillers pourront faire des analyses de votre consommation par rapport à d'autres consommateurs ayant votre profil afin de révéler les dysfonctionnements, d'en déterminer les causes (appareils défectueux ou obsolètes...) et de délivrer des conseils en conséquence ». Il pourrait être possible, à terme, d'optimiser les usages de l'énergie en fonction du moment. Par exemple, on pourrait ne pas recharger les batteries de tel appareil ou ne pas faire fonctionner tel ou tel gros appareil domestique alors qu'une pointe de consommation survient, privilégiant pour le faire une période de faible consommation.
Le compteur est conçu pour accueillir sept entrées/sorties de données non-pré-affectées. Il est techniquement possible d'y connecter différents appareils pour en assurer la supervision ou le pilotage. Mais toute utilisation de cette nature, qui repose sur une grosse masse de données, supposera un consentement express du client.

Des risques importants liés aux données traitées

Ces données peuvent aussi exciter la convoitise de cybercriminels. Savoir que la consommation énergétique a brutalement chuté peut indiquer que les habitants sont partis en vacances, laissant une plus grande possibilité de cambriolage. « S'il existe des failles de sécurité, des données fines normalement destinées uniquement au fournisseur d'énergie pourraient en effet se retrouver entre de mauvaises mains » admet Yann Padova. Mais celui-ci rappelle que dans les années 2009-2010, il existait des sites comme PleaseRobMe.com qui s'appuyait sur les publications sur les réseaux sociaux pour indiquer quelles maisons étaient vides, dans un but de sensibilisation. Les données permettant de donner des idées aux criminels ne sont donc pas réellement une nouveauté. Mais, à l'inverse, le compteur communiquant peut contribuer à améliorer la sécurité puisque une consommation d'énergie anormale pendant l'absence prévue des habitants peut indiquer la présence d'un cambrioleur.
En association avec du chantage à l'extorsion de fonds à l'égard des fournisseurs, on peut aussi imaginer des cyber-attaques déconnectant les compteurs de toute une zone géographique, provoquant de fait des coupures massives d'électricité. Yann Padova reconnaît : « comme les outillages de type Scada, le réseau électrique était classiquement totalement fermé et propriétaire d'un fournisseur unique qui était à la fois producteur et distributeur alors qu'en introduisant des outils communicants on l'ouvre largement, provoquant ainsi des vulnérabilités et des risques. » A l'inverse du compteur intelligent du gaz, Gazpar, où cette télé-fermeture/télé-ouverture de l'alimentation est physiquement impossible, elle est bien techniquement possible sur les compteurs électriques. Ces choix faits en France ne sont pas forcément les mêmes à l'étranger : l'équivalent de Gazpar en Italie dispose d'une valve télécommandée.
De ce fait, outre la CRE, divers acteurs vont surveiller attentivement le réseau électrique : la CNIL, bien sûr, qui se préoccupe des données personnelles et de leur sécurité, mais aussi l'ANSSI qui audite et certifie la couche de communication. Les distributeurs d'énergie sont en effet des Opérateurs d'Importance Vitale : un piratage aurait des répercussions à l'échelle du pays. La CRE veille, de son côté, à ce que le marché puisse bien fonctionner et donc que la confiance y règne.
Ces différents organismes veillent à émettre des bonnes pratiques telles que le *privacy by design*.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO : 40 bd Henri Sellier 92150 Suresnes
Rédacteur en chef : Bertrand Lemaire, blemaire@it-news-info.com
Tél. : 01 41 97 62 10
Principaux associés : Adthink Media et International Data Group Inc.
Président : Bertrand Gros
Directeur de publication : Bertrand Gros
Directeur général : Jean Royné
Président du groupe Adthink Media : Sylvain Morel

CIO est édité par IT NEWS INFO, SAS au capital de 3000000 €
Siret : 500034574 00029 RCS Nanterre