La sécurité des objets connectés

Par David HOZÉ (2000)

Les révolutions technologiques se succèdent et ne se ressemblent pas. Une révolution en cours répond au doux nom de IoT : « Internet of Things », ou encore les « objets connectés ».

La révolution du smartphone a ouvert la voie à celle des objets connectés

C'est probablement grâce au remplacement du téléphone mobile par les « smartphone » que les objets qui nous entourent sont en train de se transformer en « objets intelligents et connectés ». Les énormes volumes de smartphones vendus dans le monde ont entrainé une course effrénée à la miniaturisation électronique et une généralisation de l'Internet mobile, ouvrant ainsi une voie royale à l'informatisation et au raccordement à Internet des objets qui nous entourent.

Le Cabinet McKinsey estime que le marché des objets connectés va représenter en 2025 entre 5 et 7 milliards de dollars. Les principaux domaines où sont attendus ces objets sont la santé (mesure des constantes vitales, systèmes d'alerte en cas d'accident…), le sport et le bien-être (coachs sportifs, mesure des cycles du sommeil, du taux de stress…), la domotique (réfrigérateur intelligent, TV connectée, contrôle de température…) et l'automobile. L'internet mobile quant à lui se déportera peut être de l'écran des smartphones vers les lunettes ou les montres. La liste des objets connectés est impossible à dresser, car elle s'allonge tous les jours et elle est sans fin.

L'incroyable apport de ces objets connectés pour l'utilisateur et la course contre la montre que se livrent les fabricants pour sortir leurs produits repoussent au second plan les interrogations sur les risques de sécurité présentés par ces nouveaux compagnons. L'utilisateur, fortement demandeur de nouveaux services connectés pour l'aider dans sa vie au quotidien et se divertir, a déjà accepté avec le smartphone un certain niveau de risques et souvent mis de côté ses inquiétudes concernant la gestion de ses données personnelles.

Les équipements connectés et leur surface de vulnérabilités très importante

Et pourtant, cette révolution va entrainer son lot de risques et d'incidents de sécurité, qu'il sera important, voire vital, de chercher à éviter. Les premières analyses de sécurité menées sur ces équipements montrent un très grand nombre de vulnérabilités et de comportements anormaux (mots de passe triviaux, données non chiffrées transmises en clair sur Internet, interfaces mal sécurisées systèmes d'autorisation faillibles…).

Les smartphones ont pourtant apporté leur premier lot de vulnérabilités. Tout d'abord au niveau des systèmes d'exploitation, dont la fréquence de renouvellement (rarement plus de 6 mois) offre un boulevard à la découverte et l'exploitation de vulnérabilités par les hackers. Rares sont les applications anti-virus pour mobiles qui arrivent à détecter un malware ou un cheval de Troie lorsqu'il est bien caché au sein du système d'exploitation du smartphone. Les applications ensuite, qui totalement officiellement, récupèrent l'accès aux listes de contacts, aux SMS, à la ligne téléphonique, voire aux emails de l'utilisateur. Les plates-formes hardware ensuite, qui pour des raisons de « time to market » des équipementiers présentent de nombreuses vulnérabilités.

Les objets connectés arrivent avec les mêmes types de vulnérabilités que les smart-devices, permettant potentiellement le vol d'informations, la prise de main de l'équipement à distance, ou la modification des données contenues dans l'équipement…. Ils présentent par contre des scénarios de menace propres aux équipements connectés. Et ces derniers peuvent avoir de graves conséquences : détournement du système de pilotage d'une automobile, modification du dosage d'une pompe à insuline, modification d'une variable dans le carnet d'entretien d'un avion stocké dans les google glasses du technicien et utilisé lors de la maintenance d'un avion.

Même si la sécurité est un argument souvent avancé par les fabricants d'objets connectés, l'heure est pourtant essentiellement à la recherche des nouveaux usages et donc des marchés. Ainsi, Google avec son programme « Glass at Work », dont la vocation est de trouver les usages de demain pour les Google Glass dans le monde professionnel, a ouvert l'accès à ses API (interfaces informatiques) afin d'encourager les développeurs à créer les applications de demain. Ainsi, des sociétés type Aumedix, ambassadeur de Google dans le domaine de la santé, équipe déjà aujourd'hui plusieurs médecins dans des hôpitaux américains, leur permettant de consulter et de compléter les dossiers des patients en temps réel et d'afficher des informations complémentaires durant leurs opérations.

Photo libre de droits : l'auteur avec des Google Glass

Objets connectés : source de risques ou source de progrès ?

Faut-il cependant tomber dans la psychose des objets connectés et refuser les extraordinaires apports qu'ils laissent présager ? Tout d'abord, peu de personnes réussiront à éviter les objets connectés. Ces derniers vont se multiplier et il y a fort à parier que d'ici quelques années, il sera difficile de trouver une voiture sortant d'une usine qui ne soit pas connectée. Qui demande déjà aujourd'hui à son médecin de ne pas taper sa prescription sur son ordinateur et de privilégier l'ordonnance papier, par peur du piratage de l'ordinateur du médecin ?

Ensuite, la plupart des objets connectés proposeront des services dont les enjeux pour les pirates seront de faibles intérêts, et qui ne présenteront pas de risques majeurs. Pourquoi un pirate risquerait la prison en s'attaquant à un réfrigérateur connecté ou bien à une visite interactive d'un musée sur des Google glass, alors qu'il risque une peine de prison de 5 ans et des centaines de milliers d'euros d'amende ?

Les enjeux sécurité des objets connectés sont donc à lier aux usages qui vont en être faits. Il est bien sûr effrayant qu'un pirate puisse prendre la main sur un système de micro-chirurgie pendant une opération, mais dans le même temps, les objets connectés vont permettre de sauver de nombreuses vies, par exemple avec la généralisation de systèmes d'alerte en cas d'AVC pour les personnes à risques. Il n'y a donc pas d'inquiétude générale à développer face à cette révolution, mais bien des inquiétudes ciblées, en fonction des usages qui en seront faits et des risques induits.

Quant à la principale préoccupation des usagers (85% des français sont préoccupés par le détournement de leurs données personnelles – Etude CSA Février 2014), celle-ci bénéficie en France du travail de la CNIL qui définit et fait appliquer le cadre réglementaire concernant la protection des données.

Reste à l'usager à faire attention aux éventuelles demandes d'accès à ses données personnelles qui lui sont présentées par les éditeurs lorsqu'il accède à certaines applications ou certains équipements. Que pourrait faire la CNIL face à des utilisateurs qui, sans s'en rendre compte, auraient lors de l'installation de l'application autorisé une société à collecter et à partager leurs données de santé, par exemple avec des compagnies d'assurance, qui pourraient ainsi augmenter leur prime, refuser un remboursement ou refuser d'assurer un prêt ? Dans certains cas, si l'utilisateur refuse le partage de ses données personnelles, il est alors empêché d'accéder au service.

L'utilisateur et l'entreprise doivent apprivoiser intelligement les objets connectés

C'est donc bien une utilisation responsable et avertie, ainsi qu'un cadre réglementaire fortement contrôlé et applicable par tous les fournisseurs de services où qu'ils soient dans le monde, qui permettra aux utilisateurs d'être protégés des risques associés aux objets connectés. L'utilisateur doit également penser à se protéger. Par exemple, une application Smartphone permettant le contrôle via son smartphone de ses stores électriques ne nécessite pas de connaitre son nom ni son adresse postale. Question de bon sens !
En parallèle de l'accélération des cycles technologiques, et de l'explosion de la quantité des données, les équipes de sécurité informatiques en entreprise voient l'arrivée des objets connectés comme autant de de nouveaux fronts à adresser pour assurer la protection des Assets de l'entreprise. L'utilisation des objets connectés pour optimiser les processus métiers de l'entreprise la rendra certes plus agile et plus concurrentielle, mais s'il n'est pas accompagné d'une bonne démarche de sécurité, il pourrait également entrainer sa perte. Expertise sécurité et bon sens seront les maîtres mots de cette protection qui devra permettre à l'entreprise de gagner en agilité tout en maîtrisant ses risques sécurité. ▮

L'AUTEUR

David HOZÉ, Ingénieur TélécomParistech 2000, a démarré sa carrière dans les Cabinets de Conseil technologiques généralistes. Il crée en 2010 le Cabinet de Conseil WISE PARTNERS, spécialisé en sécurité de l'information et en confiance numérique, avec pour ambition de rendre la sécurité plus agile et plus efficace, au service de l'entreprise innovante. Il accompagne depuis plus de 15 ans les grandes entreprises et les administrations dans leurs démarches de gestion du risque informationnel, de sécurité informatique et de confiance numérique.
Contact : david.hoze@wise-partners.fr