L'Internet des Objets modifie la cybersécurité : l'exemple de Linky

Par **Hervé CHAMPENOIS**,
Directeur du programme Linky chez ENEDIS

Le programme Linky, un poste d'observation privilégié du développement de l'Internet des Objets

Le déploiement des compteurs d'électricité Linky s'inscrit dans un phénomène bien plus large qui est celui du développement des objets connectés dans le monde. Ce développement est si rapide que l'on peine à dénombrer précisément ces objets connectés, même si on peut aujourd'hui estimer qu'ils sont aux alentours de vingt milliards – soit trois par humain ! L'essor de l'internet des objets s'explique par le développement de la communication sans fil – la 5G va encore amplifier le phénomène –, conjugué à la transformation numérique de la sphère privée et de la sphère professionnelle, et à l'augmentation des services autour des données individuelles et collectives.

Ce mouvement touche aussi bien les objets du quotidien – les smartphones, les montres, les véhicules, les réfrigérateurs, les trottinettes électriques, les box Internet…– que les applications professionnelles. L'installation de 35 millions de compteurs communicants à horizon 2021 en est donc une illustration parmi tant d'autres. Linky apporte de nouveaux services à nos clients tout en permettant d'améliorer la gestion du réseau exploité par Enedis pour de nouveaux développements du réseau (autoconsommation avec les panneaux solaires, véhicule électrique…). Aujourd'hui, environ deux Français sur trois sont déjà équipés du nouveau compteur. Et l'appropriation est bonne : plus de 85 % des clients se disent satisfaits de Linky. Nous constatons chaque mois une progression d'environ 10 % du nombre de clients abonnés aux services associés aux nouveaux compteurs : c'est une progression similaire à celle des abonnés à la fibre par exemple, et cela dit beaucoup de l'appétence de chacun pour les usages de cet objet connecté qui est l'allié du consommateur et de la transition énergétique. Il permet par exemple de suivre sa consommation d'électricité précisément alors que par le passé, nous ne disposions au mieux que d'une mesure tous les six mois.

Le succès de l'IoT au prisme de Linky

La finalité première de l'internet des objets, c'est d'apporter de nouveaux services pour les clients et des gains d'efficacité pour les entreprises – par exemple pour optimiser le suivi des flux logistiques ou la maintenance prédictive des infrastructures. Les champs d'application sont très larges, de la santé au divertissement en passant par la maison connectée dont le marché ne cesse de progresser et représente aujourd'hui environ 2 milliards d'euros par an en France. On le voit en particulier avec le développement des véhicules en partage (scooter, voiture, trottinettes, vélo) dont l'expansion repose sur deux objets connectés : le smartphone et le véhicule loué.

Avec le nouveau compteur, Enedis, entreprise de service public implantée dans tous les territoires, modernise le réseau de distribution d'électricité et améliore la qualité du service rendu aux Français, notamment pour les accompagner vers la transition énergétique.

Prenons quelques exemples : lorsque vous vous installez dans un nouveau logement dans lequel il est nécessaire de remettre en service suite au départ de l'occupant précédent, vous pouvez

désormais disposer de votre électricité rétablie en moins de 24 heures. Avec l'ancien compteur, cela pouvait prendre jusqu'à 5 jours. Cet été, ce sont près de 700 000 emménagements qui ont été simplifiés grâce à la mise en service à distance. Autre exemple : les pannes sont détectées plus rapidement ce qui permet de déclencher une opération de maintenance, parfois même avant que le client ne se rende compte que l'alimentation a été coupée ! Cette réactivité est notamment indispensable lorsqu'Enedis intervient pour rétablir l'électricité suite à une tempête ou autres événements climatiques de plus en plus fréquents. Les fournisseurs d'énergie peuvent également proposer aux consommateurs des offres plus avantageuses et mieux adaptées à leurs habitudes de consommation d'électricité. Enfin, avec Linky, nos clients peuvent s'engager à leur rythme dans la transition énergétique, en suivant – et donc en maîtrisant – au plus près leurs consommations ou encore en contribuant au développement des énergies renouvelables, par exemple à travers l'installation facilitée de panneaux photovoltaïques sur le toit de l'habitation pour consommer leur propre électricité.

Tous ces changements sont synonymes de simplicité et d'économies pour le client. Ils contribuent à faciliter la vie des gens ; cela explique le caractère attractif de l'Internet des Objets.

Une condition semble néanmoins indispensable pour que les clients adhèrent à ces nouvelles possibilités, c'est qu'ils aient confiance dans notre capacité à protéger leurs données et à garantir l'intégrité des infrastructures d'Enedis – réseau de distribution et systèmes d'information – en réponse à des cyberattaques. Les services apportés par l'internet des objets ne doivent pas occulter les nouveaux enjeux en matière de cybersécurité que soulève le développement de l'IoT.

L'Internet des Objets renforce-t-il l'exposition aux cyberattaques ?

La multiplication des objets connectés reliés à des systèmes plus ou moins centralisés conduit à multiplier le nombre de points d'entrée potentiels dans les systèmes des entreprises et des administrations. Prenons un exemple simple : en se connectant au matériel d'un client, des *hackers* peuvent remonter jusqu'aux systèmes du fabricant grâce aux informations que le matériel transmet quotidiennement. La corruption de l'ensemble de l'entreprise, de ses produits et réseaux peut s'effectuer en quelques heures, voire quelques minutes. Nous avons également en tête cette expérience menée en 2015 par des chercheurs américains qui ont développé un outil pour prendre le contrôle à distance d'une voiture connectée. Tout ceci peut attirer des *hackers* car les automobiles sont en train de se transformer en « smart cars » connectées.

Les cyberattaques qui passent par les objets connectés poursuivent en fin de compte les mêmes finalités que les cyberattaques classiques – accéder à des informations confidentielles, modifier des données à des fins malveillantes ou encore bloquer des systèmes d'information et les activités associées – mais leurs effets peuvent s'en trouver démultipliés. Avant, seuls les terminaux informatiques permettaient d'accéder aux systèmes d'information ; aujourd'hui certains objets connectés utilisés au quotidien, comme les smartphones, peuvent garder la mémoire précise des faits et gestes. Les informations collectées sont nombreuses et indiquent par exemple l'emplacement physique où se trouve l'objet connecté généralement associé à la personne qui l'utilise – même si cela doit être relativisé en ce qui concerne Linky, qui par défaut ne transmet à Enedis que la consommation à une maille quotidienne et ne peut distinguer les différents usages électriques à l'intérieur de l'habitation. L'internet des objets doit donc être accompagné de mesures permettant de réduire l'exposition aux cyberattaques, mais également leurs effets potentiels.

Enedis n'a pas attendu Linky pour intégrer les exigences les plus élevées en matière de cybersécurité. Les réseaux de distribution d'électricité sont en effet des infrastructures qui nécessitent une protection à la hauteur des enjeux associés.

IoT et cybersécurité : un changement de perspective

La cybersécurité repose sur trois grands piliers : la protection par conception des matériels, logiciels et canaux de communication, la surveillance de sécurité, et la capacité de réaction aux agressions. Pour autant le rôle et le comportement des utilisateurs demeurent cruciaux. Cette approche se décline naturellement sur l'internet des objets mais avec une amplification liée au champ d'application qui englobe une multitude d'objets et d'utilisateurs. C'est ce qui la rend plus large et plus exigeante en matière de réactivité.

Avec la démultiplication des objets connectés, il ne s'agit plus seulement de protéger et de défendre la « place forte » que représente le système d'information centralisé, mais également les faubourgs et la campagne environnante : la surveillance doit donc être adaptée, et nécessite une attention permanente. Cela implique de sécuriser l'objet connecté mais également les logiciels informatiques qui constituent le support de transmission, de stockage et de traitement de l'information. L'effort doit se concentrer alors dans la capacité à mettre sur le marché des objets modernes, performants tout en garantissant une protection adaptée à leurs usages dans un contexte de forte concurrence. L'ETSI (*European Telecommunications Standard Institute*) a par exemple récemment publié des standards techniques de base pour la sécurité de l'IoT, c'est une bonne chose qui traduit la prise en main du sujet « cybersécurité » dans le domaine des objets connectés.

Par ailleurs, dès lors que l'objet connecté est installé, sa supervision et la mise à jour des logiciels pour apporter des correctifs dans une logique de conformité représente un défi, à la fois parce que ces objets sont répartis dans de vastes espaces, mais aussi parce que le coût des mises à jour – et *a fortiori* des contrôles sur site – est significatif par rapport au coût unitaire de l'objet.

Ensuite, parce que la démultiplication des objets s'accompagne d'une démultiplication des utilisateurs. Toute personne qui possède un objet connecté doit être considérée comme partie prenante du processus global de sécurité. La sensibilisation des utilisateurs est donc un enjeu majeur, elle passe souvent par des choses simples – avoir un mot de passe suffisamment long, éviter de se connecter autant que possible sur des réseaux sans fil inconnus… – mais le nombre d'utilisateurs rend la tâche plus ardue. Cette sensibilisation vaut aussi bien pour le grand public que pour les salariés d'entreprises et d'administrations qui ont à traiter de plus en plus de données confidentielles. Elle nécessite d'adapter les processus internes et d'accompagner chaque utilisateur de données. Chez Enedis, nous avons par exemple mis en place un module pédagogique « conformité RGPD » que chaque salarié est tenu de suivre.

Répondre à ces nouveaux défis : l'exemple du déploiement de Linky

A l'aune de l'expérience Linky, trois axes nous semblent incontournables pour profiter des services qu'offrent les objets connectés tout en assurant le niveau le plus élevé possible de cybersécurité.

En premier lieu, la sécurité doit être pensée dès la conception de l'objet connecté. C'est l'approche *security by design*, que l'on pourrait traduire assez simplement par « mieux vaut prévenir que guérir ». C'est ce principe que nous avons appliqué pour construire le système Linky, pour garantir aussi bien la sécurité des données de nos clients que l'intégrité des infrastructures d'Enedis. Ce système est un tout qui va des compteurs jusqu'à nos systèmes d'information. A chaque niveau, des dispositifs anti-intrusion extrêmement robustes ont été prévus. La communication des données entre chaque partie est par ailleurs sécurisée à travers divers processus de chiffrement, et nos systèmes d'information sont isolés pour parer tout risque de contagion. Nous appliquons de surcroît un principe fondamental qui est au cœur de la doctrine de la CNIL (Commission nationale Informatique et Libertés) en matière

de protection des données : il s'agit du principe de proportionnalité. Les informations enregistrées et transmises par le compteur Linky sont strictement nécessaires au regard de la finalité de la collecte, qui est le comptage de consommations d'électricité. Autrement dit, les informations transmises par le compteur sont volontairement limitées et ne donnent que le minimum d'informations nécessaires sur le point de livraison en électricité. Ainsi, aucune autre information n'est véhiculée, ce qui d'ailleurs alourdirait inutilement le système.

En second lieu, la cybersécurité appliquée au domaine de l'IoT implique une approche dynamique car le contexte d'un jour n'est pas celui du lendemain. Cela demande de mobiliser des moyens importants – nous consacrons une part significative de nos efforts à la cybersécurité. Cette approche dynamique repose sur un système de supervision des objets connectés et d'audit efficace pour identifier toute amélioration et lancer d'éventuels correctifs. C'est pour cette raison que nous avons mis en place un service qui veille, 24 heures sur 24, au bon fonctionnement de cette chaîne communicante, en particulier pour détecter et juguler d'éventuels défauts. Nos équipes recherchent par ailleurs en permanence les évolutions à apporter dans le système. Si besoin, une mise à jour des mesures de protection peut être mise en place. Dans la même logique, des audits indépendants sont régulièrement menés dans nos infrastructures, à notre initiative ou à celle de nos parties prenantes, comme la CNIL ou l'Agence nationale de Sécurité des Systèmes d'Information (ANSSI).

Un dernier point nous semble fondamental, c'est que plus que jamais, avec l'essor des objets connectés, l'approche de la cybersécurité doit être collective et co-construite. Nous avons élaboré notre système de sécurité Linky en étroite collaboration avec la CNIL et l'ANSSI, qui nous délivre des certificats de conformité. Nos constructeurs sont associés à cette démarche car les chaînes de production doivent également être robustes en matière de cybersécurité, et nous communiquons en toute transparence auprès de nos clients pour leur expliquer l'usage qui est fait de leurs données et la façon dont elles sont protégées. Le tout sous l'œil des pouvoirs publics qui ont un rôle central à jouer pour créer un cadre juridique protecteur des informations et des systèmes – en particulier les plus stratégiques pour le pays –, mener des audits sur le terrain et sensibiliser la diversité des utilisateurs d'objets connectés, notamment le grand public.

Ces trois conditions doivent, nous semble-t-il, être réunies pour que l'Internet des Objets puisse effectivement concilier nouveaux services aux clients et aux entreprises, et protection de l'information. La protection efficace et démontrée de l'information représente un challenge passionnant et exigeant pour disposer de ces nouvelles technologies en toute sérénité.