Communiqué de presse ACN
27 février 2019

Cybersécurité des objets connectés : le référentiel récemment proposé par l'ETSI constitue un premier pas nécessaire mais pas suffisant !

Dans un monde où les objets connectés se multiplient de manière exponentielle et où, pour l'heure, la cybersécurité n'est pas toujours intégrée dès la conception de ces objets, l'initiative de l'ETSI (European Telecommunications Standard Institute) de publier des spécifications techniques de base pour l'IoT est une véritable avancée.

Cependant, pour certains objets connectés pouvant être utilisés dans des applications nécessitant un plus grand niveau d'assurance, il est impératif de compléter ces règles minimales par des procédures plus robustes en termes d'exigences de cybersécurité. Des travaux sont en cours par les entreprises de la filière cybersécurité, au sein de l'Alliance pour la Confiance Numérique en France et d'Eurosmart en Europe, pour définir des spécifications et les tests associés permettant d'attester d'un niveau d'assurance plus élevé pour les objets connectés.

L'ACN salue la récente publication des spécifications techniques ETSI 103 645 relatives à la cybersécurité dans l'internet des objets. Ces spécifications concernent la sécurité d'objets de consommation connectés à une infrastructure de réseau, telle qu'internet ou un réseau domestique. Elles englobent un large panel d'objets connectés, des jouets pour enfants, aux enceintes intelligentes, en passant par les détecteurs de fumée (liste non exhaustive). Cette publication répond à un besoin croissant de cybersécurité dans un secteur IoT en pleine expansion mais encore peu préparé aux cyber-risques. *« Ces spécifications effectuent un bon recensement des règles de cybersécurité minimales que tout concepteur d'IoT devrait suivre dans un monde où la cybermenace se fait toujours plus présente. En effet, les objets connectés, du fait de leur grand nombre et de leur sécurisation quasi inexistante sont non seulement des cibles potentielles mais aussi des vecteurs permettant notamment des cyberattaques de type DDoS (Déni de Service Distribué). Ces règles d'hygiène, si elles sont largement appliquées, rendraient ce type d'attaques plus difficiles et plus coûteuses à réaliser »* se félicite Jean-Pierre Quémard, Président de l'ACN.

Les spécifications ETSI 103 645 condamnent l'utilisation de mots de passe universels par défaut et préconisent la mise en place d'une politique de divulgation coordonnée de vulnérabilités. De multiples dispositions sont consacrées aux mises à jour des logiciels, qui doivent être aussi régulières que nécessaire. *« Toutes ces dispositions relèvent de l'hygiène informatique que tout objet intégrant de la connectivité doit suivre à minima. Ces principes de base sont bien sûr nécessaires et leur application généralisée réduirait considérablement les expositions aux risques, pour autant, elles doivent être comprises comme un premier pas vers une véritable logique de cybersécurisation »,* souligne Jean-Pierre Quémard.

L'ACN accueille également favorablement l'inclusion d'un article sur la protection des données. Ces spécifications sont ainsi susceptibles d'aider les fabricants à offrir des produits IoT conformes au Règlement général sur la protection des données (RGPD). En effet, cybersécurité et protection des données personnelles vont de pair et doivent être intégrées dès la conception des produits.

Contact presse: Yoann KASSIANIDES – ykassianides@confiance-numerique.fr – 06.26.78.57.55

Ces nouvelles spécifications s'inscrivent dans un contexte de prise de conscience de l'augmentation exponentielle des cyber-risque, qui a notamment conduit à la proposition de *Cybersecurity Act* au niveau européen. Le *Cybersecurity Act,* en cours d'adoption, prévoit la création d'un cadre européen de certification de cybersécurité et définit trois niveaux d'assurance assortis d'exigences différentes : élémentaire, substantiel, élevé. L'ACN souligne que les futurs schémas de certification devront faire référence aux normes et spécifications techniques existantes afin d'être en adéquation avec le marché. Le travail réalisé par les organisations de normalisation, notamment ETSI TC Cybersecurity et CEN-CENELEC JTC13, devrait fortement inspirer la certification européenne.

Néanmoins, l'ACN tient à souligner que les spécifications proposées par l'ETSI n'apportent une réponse que pour le niveau d'assurance basique, au sens du projet de règlement européen, et ne sauraient être suffisantes pour les niveaux substantiel ou élevé. En effet, de nombreuses dispositions de ces spécifications ne sont pas des exigences obligatoires, notamment celles relatives à la mise à jour des logiciels et celles liées à la divulgation de vulnérabilités. L'ACN note également que le chiffrement des données est simplement recommandée, et seulement pour les données sensibles. En outre, ces spécifications n'incluent pas de tests de cyberattaque, tels *les* tests de pénétration, seuls à mêmes de garantir un réel niveau de sécurité correspondant aux niveaux substantiel ou élevé.

Un travail complémentaire doit donc être désormais entrepris pour tous les objets connectés qui nécessiteront un niveau d'assurance plus élevé et avec une procédure plus robuste de certification. C'est le cas par exemple des systèmes d'alarme et des enceintes intelligentes sur lesquelles une cyberattaque pourrait avoir un impact conséquent en termes de sûreté, sécurité et de respect de la vie privée.

A propos de l'ACN :

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014). L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement à ce titre aux travaux du Comité Stratégique de filière des Industries de Sécurité. Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

Contact presse: Yoann KASSIANIDES – ykassianides@confiance-numerique.fr – 06.26.78.57.55