COMPRENDRE LA CYBERSÉCURITÉ DES OBJETS CONNECTÉS.

Les objets connectés sont vulnérables, dès lors qu'ils contiennent du code. Un rapport de l'OCDE de février 2021 analyse la sécurité des produits connectés, du gadget au smartphone. Cette publication recherche l'origine des défaillances et propose des politiques visant à renforcer la sécurité des objets.

Village de la Justice - 25 mai 2021
Sabine Marcellin

Nos sociétés reposent de plus en plus sur des produits intelligents, c'est-à-dire des produits qui contiennent du code et peuvent se connecter.
Du bracelet électronique à la voiture communicante, des équipements médicaux aux caméras de surveillance, les usages connectés sont multiples.
En France, une photographie des usages en 2020 , semble conforme aux statistiques mondiales, c'est-à-dire que ces usages se concentrent principalement sur la maison connectée (50%). D'autres utilisations viennent ensuite, comme le travail (25 %), la voiture connectée (7%) et 18% d'autres applications.
Estimer le nombre d'objets connectés ou IoT (internet of Objects) est un art délicat. En effet, certains cabinets de prospective estiment les seuls objets, alors que d'autres agrègent tous les objets communicants, y compris les téléphones, ordinateurs et tablettes. Ce qui explique que Gartner prévoyait 26 milliards d'objets en 2020 et IDC jusqu'à 212 milliards.

Le constat d'une cybersécurité des IoT défaillante.

Selon le rapport de l'OCDE de février 2021 , les produits connectés présentent souvent un niveau de sécurité numérique insuffisant, résultant de lacunes qui peuvent apparaître à différentes étapes de leur cycle de vie.
Les failles de sécurité numérique s'expliquent, selon ce rapport, par une incitation insuffisante à intégrer la sécurité, une répartition peu claire des responsabilités entre acteurs et un manque de coopération entre parties prenantes et agences gouvernementales.
En conséquence, il y a un manque de respect des directives et normes volontaires (ISO, etc.) pour la sécurité par conception et la sécurité par défaut et le traitement des vulnérabilités nouvellement découvertes est souvent sous-optimal.
Le rapport souligne un risque particulier en fin de vie des produits intelligents. En effet, ceux-ci continuent souvent d'être utilisés, alors qu'ils ne sont plus pris en charge par les mises à jour de sécurité. Cet écart de fin de vie, entre la fin du support de sécurité et la fin de l'utilisation, doit être comblé. Avec des milliards de produits IoT atteignant leur fin de vie dans la décennie à venir, la possibilité d'un « *internet des objets oubliés* » représente pour l'OCDE un défi politique imminent.
Afin d'améliorer la sécurité des IoT, l'OCDE propose la mise en œuvre de principes politiques à destination des décideurs politiques et des parties prenantes.

Les principes de haut niveau pour améliorer la sécurité numérique des produits

Pour relever ces défis, le rapport décrit six principes de haut niveau qui peuvent guider l'action des acteurs :

- Accroître la transparence et le partage d'informations, afin de remédier aux asymétries d'informations, y compris pour la traçabilité des composants des produits intelligents ;
- Sensibiliser et responsabiliser les parties prenantes, en particulier les utilisateurs finaux et les chercheurs en sécurité ;
- Assurer la responsabilité et le devoir de diligence des offreurs de produits, selon cinq sous-principes : sécurité dès la conception (security by design), sécurité par défaut (security by default), gestion dynamique de la sécurité, politiques de fin de vie responsables et réparabilité ;
- Renforcer la coopération entre acteurs, agences gouvernementales et au niveau international ;
- Promouvoir l'innovation et la concurrence ;
- Aborder la sécurité numérique avec proportionnalité, à travers une approche basée sur les risques, pour prendre en compte la complexité.

Une boîte à outils politique : « *des politiques intelligentes pour des produits intelligents* ».

Les produits intelligents nécessitent des politiques intelligentes pour la sécurité numérique. L'OCDE recommande que les décideurs politiques intègrent la cybersécurité des IoT dès le développement de produits, par un processus centré sur l'utilisateur final.
Si ces mécanismes échouent, alors l'utilisation d'instruments réglementaires plus stricts, tels que des exigences légales, pourrait être étudiée plus avant.
De même, les ingénieurs en logiciel peuvent également apprendre des décideurs. Équilibrer les intérêts des différents groupes de parties prenantes, prendre en compte l'impact de leurs décisions sur les autres et prendre en compte le long terme devrait devenir une partie inhérente du cycle de développement des produits intelligents.
Une stratégie visant à améliorer la sécurité numérique des produits nécessitera probablement une combinaison d'outils politiques pour être plus efficace. La boîte à outils politique décrite dans le rapport vise à permettre aux gouvernements de favoriser l'adoption des principes de haut niveau, en se concentrant sur le « comment » plutôt que sur le « *quoi* ».

Les outils proposés par l'OCDE sont les suivants :

- Sensibiliser les utilisateurs traditionnels et développer les compétences en sécurité numérique afin de développer la main-d'œuvre experte des utilisateurs avancés ;

- Au-delà de leur rôle de régulateurs, les gouvernements sont également des agents économiques. A ce titre, ils peuvent tirer parti de leur pouvoir d'achat et montrer l'exemple. Grâce aux politiques de marchés publics, ils peuvent inciter les acteurs du côté de l'offre à certifier la sécurité numérique des produits intelligents ;

- Les normes techniques sont également primordiales. Développées par le gouvernement ou la communauté multipartite, ils fournissent aux offreurs des orientations claires, qui peuvent être adaptées à chaque marché ou catégorie de produit spécifique ;

- Les labels pourraient inciter les acteurs du côté de l'offre à adhérer aux normes et contribuer à réduire les asymétries d'information. Depuis novembre 2020, la Finlande, l'Allemagne et le Japon ont lancé ou envisagent de lancer des systèmes d'étiquetage de sécurité numérique pour des catégories de produits spécifiques, telles que l'IoT grand public ou les routeurs. Cependant, la lassitude des consommateurs et le manque d'adoption par l'industrie doivent être considérés comme des inconvénients potentiels des initiatives d'étiquetage ;

- L'efficacité des dispositifs juridiques doit être évaluée plus avant. Bien que le code soit partout, les produits intelligents sont relativement nouveaux et ne correspondent pas nécessairement aux catégories juridiques du 20e siècle. L'application aux IoT des lois, des assurances et des garanties en matière de responsabilité est difficile et nécessitera probablement un examen des cadres existants pour les adapter à la dynamique complexe de l'économie numérique ;

- Enfin, certains pays de l'OCDE s'intéressent de plus en plus à l'élaboration de réglementations plus strictes afin d'améliorer la sécurité numérique des produits. Des exigences techniques aux principes de haut niveau, ces réglementations pourraient être efficaces pour garantir le devoir de diligence des fabricants. Le rapport examine les opportunités et les défis associés et fournit des informations clés, par exemple en ce qui concerne le besoin de neutralité technologique, de proportionnalité et de coopération internationale.

La coopération internationale est essentielle.

Il est essentiel que les décideurs politiques adoptent une approche holistique de la sécurité numérique des produits. C'est le moment pour les gouvernements, selon l'OCDE, de concevoir des politiques intelligentes pour les produits intelligents, d'être proactifs plutôt que réactifs, et de façonner l'environnement politique pour la sécurité numérique des produits avec prévoyance.
À cet égard, la coopération internationale apparaît comme un facteur clé de succès. Pour les décideurs, il est essentiel de tirer les leçons des succès et des défis des autres pays et de tirer parti des politiques qui ont déjà fait leurs preuves ailleurs. Certaines politiques de pointe développées au niveau national ont formé la base de normes internationales émergentes : un code de pratique développé par le gouvernement britannique a ouvert la voie à la spécification technique de l'ETSI pour la sécurité IoT des consommateurs.
La coopération internationale est également essentielle pour permettre l'interopérabilité entre les approches nationales, éviter la prolifération des normes et limiter les incohérences entre les juridictions, ce qui pourrait entraver considérablement le développement de l'économie numérique.