Appareils connectés et cybersécurité : l'UE passe à l'Act !

© Blue Planet Studio / Adobe Stock

Permettre à toutes sortes d'appareils de se connecter de manière non sécurisée rend les réseaux vulnérables, surtout lorsque ces appareils n'y sont pas autorisés. À l'inverse, ces appareils connectés risquent d'être « pris en charge » par des réseaux non autorisés et de devenir la cible d'attaques ou de manœuvres frauduleuses. Pour remédier à cela, des mécanismes fiables, évolutifs et automatiques sont nécessaires pour gérer en toute sécurité les appareils connectés tout au long de leur cycle de vie : c'est à cela que s'est attelée l'Union européenne au travers du futur « Cyber Resilience Act »[1].

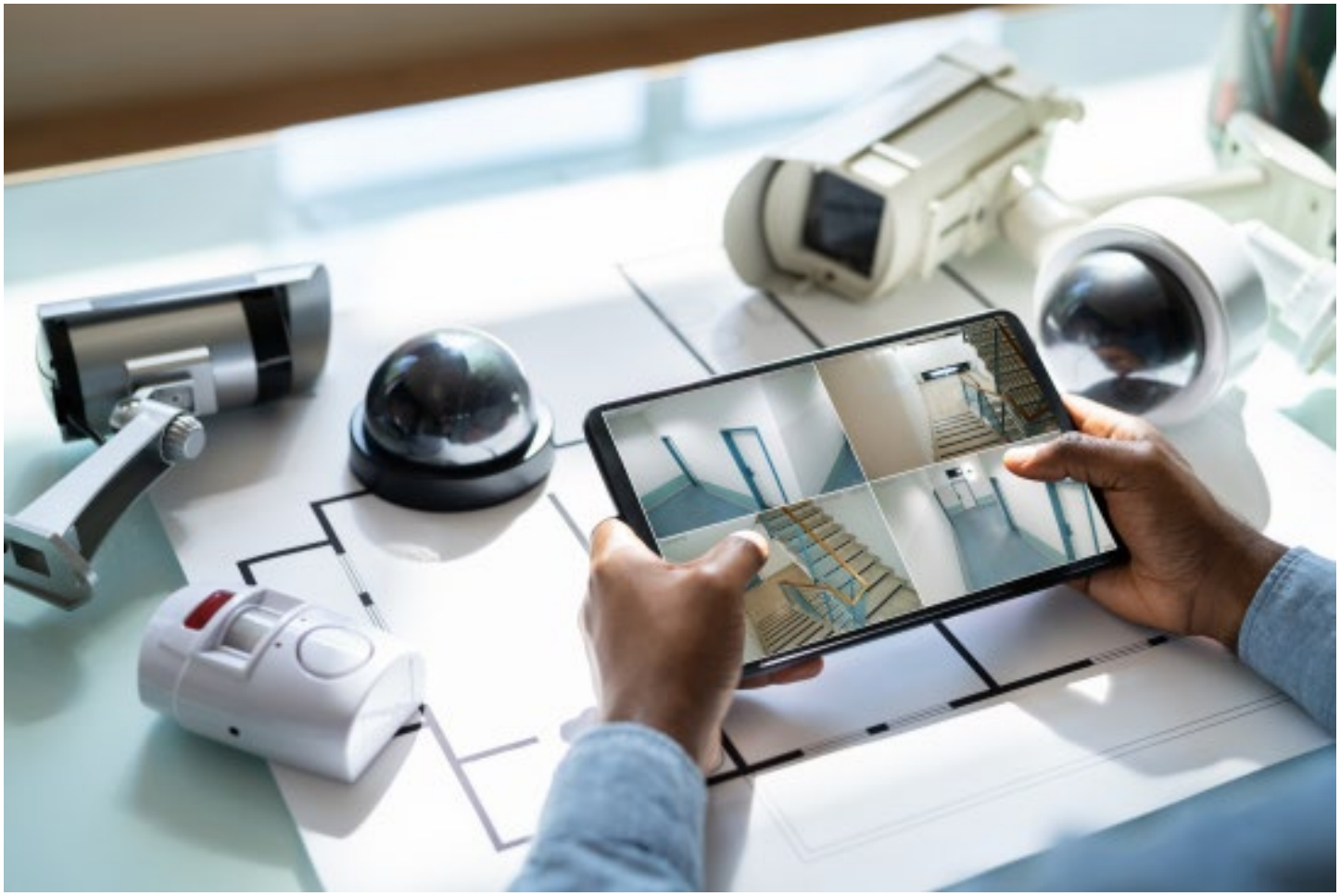
Rien ne sert de se voiler la face : de nombreux produits connectés présentent un faible niveau de sécurité informatique. Régulièrement, ANPI vous tient informés de cette situation[2]. En outre, nombre de producteurs ne fournissent pas de mises à jour pour remédier aux vulnérabilités de leurs produits. Ces vulnérabilités ont un coût lorsque la sécurité est défaillante, tant pour les consommateurs que pour les utilisateurs professionnels. Ceux-ci ne disposent souvent pas d'informations suffisantes et précises lorsqu'il s'agit de choisir des « produits sûrs » et de s'assurer que ceux-ci sont configurés de manière sécurisée.

Le principe général de base qui préside à la réglementation européenne est que seuls peuvent être commercialisés dans les États membres des produits « sûrs »[3].

1 *Acte législatif sur la cyber-résilience (voir référence en fin d'article).*

2 *Quand les objets connectés deviennent inutilisables / Jeanine Driessens - Fire & Security Alert Magazine n° 18, mars 2020, p. 79 ; Les caméras de surveillance ne sont pas toujours sûres / Fire & Security Alert Magazine n° 16, septembre 2019, p. 52-53.*

3 *Produit sûr : « tout produit qui, dans des conditions d'utilisation normales ou raisonnablement prévisibles, y compris de durée et, le cas échéant, de mise en service, d'installation et de besoins d'entretien, ne présente aucun risque ou seulement des risques réduits compatibles avec l'utilisation du produit et considérés comme acceptables dans le respect d'un niveau élevé de protection de la santé et de la sécurité des personnes. […] » (Code de droit économique, art. I.10).*



© Andrey Popov / Adobe Stock

Transposé en matière de cybersécurité, cela signifie que le produit doit entre autres :

- être conçu et réalisé de manière à offrir un niveau de sécurité adapté aux cyberrisques liés à son utilisation ;
- ne pas comporter de vulnérabilités connues au moment où il est vendu ;
- présenter une configuration sécurisée par défaut ;
- être protégé contre les connexions illicites ;
- assurer la protection des données qu'il recueille ;
- ne collecter que les données nécessaires à son fonctionnement.

PROPOSITION DE RÈGLEMENT EUROPÉEN

L'actualité montre quotidiennement qu'il est essentiel de renforcer la réponse aux cyberattaques et d'harmoniser la cybersécurité au niveau européen, et par ruissellement aux niveaux nationaux.

La Commission européenne a par conséquent introduit une proposition de règlement relative à une législation sur la cyber-résilience (« Cyber Resilience Act » - CRA)[4], visant à établir des normes de cybersécurité plus élevées afin :

- de créer un système fiable pour les opérateurs économiques, et
- de garantir aux citoyens de l'Union européenne une utilisation sûre des produits sur le marché.

Cette proposition sur la cyber-résilience concerne pratiquement tous les produits numériques (produits comportant des éléments numériques et logiciels), à l'exclusion de ceux qui sont de nature médicale ou concernent l'aviation civile, les véhicules et les produits conçus à des fins militaires.

QUATRE OBJECTIFS

Cet instrument législatif poursuit essentiellement quatre objectifs :

- veiller à ce que les fabricants améliorent la sécurité des produits comportant des éléments numériques, au cours de la phase de conception, de développement et tout au long de leur cycle de vie ;
- garantir un cadre cohérent de règles en matière de cybersécurité, en facilitant le respect des règles par les fabricants de matériels et de logiciels ;
- améliorer la transparence des dispositifs de sécurité des produits comportant des éléments numériques ;
- et, enfin, permettre aux entreprises et aux consommateurs d'utiliser ces produits en toute sécurité.

4 *Voir référence en fin d'article.*

En substance, la proposition introduit un marquage CE en matière de cybersécurité, en prescrivant qu'il soit apposé sur tous les produits couverts par et conçus conformément à la législation.

PRODUITS VISÉS

Comme mentionné plus haut, la définition des *« produits comportant des éléments numériques »* est très large et couvre tout produit logiciel ou matériel, ainsi que tout logiciel ou matériel non incorporé dans un produit mais commercialisé séparément.

La proposition introduit des exigences obligatoires en matière de cybersécurité tout au long du cycle de vie des produits comportant des éléments numériques, mais elle ne remplace pas celles qui existent déjà. Au contraire, les certificats des produits qui ont déjà été certifiés conformes à des normes de l'Union préexistantes resteront valides au sens du nouveau règlement.

La législation sur la cyber-résilience prévoit une macro-catégorie de produits et logiciels dits « normaux » pour lesquels il est possible de s'appuyer sur une auto-évaluation du fabricant, comme il en va déjà pour d'autres types de certification portant le marquage CE. Selon la Commission, 90 % des produits sur le marché relèvent de cette catégorie. Les produits concernés peuvent être mis sur le marché après auto-évaluation de leur cybersécurité par le fabricant. Celui-ci fournit une documentation appropriée telle qu'établie par les lignes directrices de la réglementation.

Les produits qui font partie des 10 % restants sont répartis en deux autres catégories :

- la classe I pour les produits « les moins dangereux » ;
- la classe II pour « les plus dangereux », dont la mise sur le marché nécessite une attention accrue.

Il s'agit de *« produits critiques comportant des éléments numériques »*, dont la défaillance peut provoquer d'autres atteintes dangereuses et plus étendues en matière de sécurité (les catégories de produits concernés sont énumérées dans une annexe de la proposition).
Pour les produits relevant de ces deux classes, les autocertifications de base ne sont admissibles que si le fabricant démontre qu'il a respecté des normes de marché spécifiques et des spécifications de sécurité ou des certifications de cybersécurité déjà prévues par l'Union européenne. Dans le cas contraire, il peut obtenir la certification du produit par un organisme de certification accrédité dont l'attestation est obligatoire pour les produits de classe II.

CERTIFICATION, SURVEILLANCE DU MARCHÉ ET SANCTIONS

Des normes élevées jouent un rôle essentiel pour mettre en place un système solide de cybersécurité de l'Union européenne pour tous les opérateurs économiques, et qui serve à garantir aux consommateurs de pouvoir utiliser en toute sécurité chaque produit mis sur le marché et à renforcer leur confiance dans le monde numérique.

Les importateurs et les distributeurs seront tenus de vérifier la conformité du fabricant avec les procédures pertinentes et le marquage CE du dispositif. Les fabricants de produits critiques de classe I et II devront suivre une procédure spécifique de mise en conformité. Pour les appareils de classe II, une expertise réalisée par une tierce partie est requise (organisme de certification).

Les autorités nationales compétentes devront suivre une liste d'exigences pour mettre en place des organismes notifiés qui assureront les évaluations par des tiers, et mettre en place des organismes de surveillance du marché (par exemple les autorités de cybersécurité). Elles pourraient effectuer des

© Bro Vector / Adobe Stock

© ryanking999 / Adobe Stock

opérations « coup de balai », c'est-à-dire des contrôles simultanés et coordonnés de certains dispositifs afin de vérifier leur conformité. En cas de non-conformité, les autorités nationales pourront interdire le produit sur le marché européen. Un régime de sanctions sera également prévu.

UN COMPROMIS ?

Comme toute législation en cours de développement, cette proposition de règlement est susceptible de subir modifications et amendements : récemment, un compromis a d'ailleurs été présenté par la Suède qui assure actuellement la présidence tournante du Conseil de l'UE.

L'annexe identifiant les classes de produits critiques pourrait être remplacée par des critères.

Le premier critère consisterait à déterminer si le produit possède *« une fonctionnalité liée à la cybersécurité et, en particulier, s'il exécute principalement des fonctions essentielles à la sécurité, notamment la sécurisation de l'authentification et de l'accès, la prévention et la détection des intrusions, la sécurité des points terminaux ou la protection des réseaux »*.

Le deuxième critère consisterait à déterminer si le produit remplit une fonction de système central, telle que la gestion de réseau, le contrôle de la configuration, la virtualisation, le traitement des données personnelles ou toute autre fonction susceptible de perturber de nombreux appareils connectés.

Des exigences essentielles supplémentaires sont également introduites (identifiant de produit unique, suppression des données et des paramètres du produit pour son élimination en toute sécurité, analyse des risques de cybersécurité sur base de la fonction prévue et de l'utilisation raisonnablement prévisible, ainsi que des conditions spécifiques d'utilisation).

Il faudra bien entendu rester à l'écoute des futurs développements : inspirer confiance dans les technologies utilisées par les produits connectés constituera un véritable défi...

Christopher BOON
ANPI - Information, Marketing & Communication

Référence : *Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 [COM(2022) 454]*

POUR SUIVRE L'ÉVOLUTION LÉGISLATIVE :

- *Acte législatif sur la cyber-résilience - Procédure 2022/0272 (COD)*
  https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=fr

À CONSULTER :

- *Position Paper on proposed Cyber Resilience Act / Euralarm, 20 January 2023*
  https://www.euralarm.org/resource/euralarm-releases-position-paper-on-cyber-resilience-act.html
- *La présidence suédoise du Conseil de l'UE présente la première révision complète de la législation sur la cyberrésilience / Luca Bertuzzi - EURACTIV.com, 26 avril 2023*
  https://www.euractiv.fr/section/economie/news/la-presidence-suedoise-du-conseil-de-lue-presente-la-premiere-revision-complete-de-la-legislation-sur-la-cyberresilience/