Cyber-rÃ©silience de lâ□□IoT : Loi europÃ©enne.!
Internet
PostÃ© par : JulieM
PubliÃ©e le : 14/9/2022 13:00:00

Les objets connectÃ©s sont souvent considÃ©rÃ©s comme le maillon faible de la cybersÃ©curitÃ© au sein des entreprises, il n'est donc pas surprenant que l'Union EuropÃ©enne discute dans les prochains jours d'une proposition de loi dans le cadre du Cyber Resilience Act.Â

L'objectif est d'Ã©tablir des normes de cybersÃ©curitÃ© et des procÃ©dures d'Ã©valuation de conformitÃ© plus strictes pour les objets connectÃ©s.

Selon Ilona Simpson, DSI EMEA chez Netskope, une telle rÃ©glementation est nÃ©cessaire, mais doit Ãªtre rÃ©flÃ©chie en dÃ©tail, et sa mise en place doit tenir compte de la capacitÃ© de l'Ã©cosystÃ¨me industriel - dont la fabrication, la supply chain et la vente au dÃ©tail - Ã l'adopter :

Â« Des tÃ©lÃ©viseurs aux montres, aux rÃ©frigÃ©rateurs, aux ampoules ou encore aux machines Ã cafÃ©, il semble que tout objet doit Ãªtre dÃ©sormais connectÃ© pour Ãªtre commercialisable.

Tous ces appareils rejoignent alors un environnement IoT en croissance exponentielle. Le problÃ¨me est que ce secteur n'a dÃ» se conformer Ã aucune rÃ©glementation en matiÃ¨re de cybersÃ©curitÃ© Ã date, et les cybercriminels le savent bien, puisqu'ils ont menÃ© par le passÃ© des attaques significatives ; en exploitant par exemple des machines Ã cafÃ© pour atteindre les rÃ©seaux informatiques dâ□□entreprises, auxquels ces appareils Ã©taient connectÃ©s.

Des normes de cybersÃ©curitÃ© de base pour tous les appareils connectÃ©s, ainsi que des procÃ©dures d'Ã©valuation de conformitÃ© plus strictes pour les produits critiques, sont donc indispensables.Â

Mais cette proposition soulÃ¨ve de nombreuses questions : sâ□□il est bÃ©nÃ©fique que les Ã©diteurs aient Ã Ã©valuer la sÃ©curitÃ© des objets connectÃ©s sur le point d'Ãªtre commercialisÃ©s, qu'en est-il des produits dÃ©jÃ prÃ©sents sur le marchÃ© ?Â

Et quâ□□adviendra-t-il si cela coÃ»te trop cher pour que les petits fabricants le fassent de maniÃ¨re rÃ©flÃ©chie ?

De plus, dans lâ□□Ã©ventualitÃ© oÃ¹ les vulnÃ©rabilitÃ©s connues des appareils connectÃ©s seront listÃ©es, les consommateurs et les entreprises devront Ãªtre sensibilisÃ©s, afin dâ□□Ãªtre en mesure de faire des choix Ã©clairÃ©s en fonction des informations partagÃ©es et des risques induits.Â

Du cÃ´tÃ© de l'offre, les organisations seront confrontÃ©es non seulement au dÃ©fi de concevoir, acquÃ©rir, mettre en Å□uvre et dÃ©ployer une pile technologique adÃ©quate, mais Ã©galement de s'assurer qu'elles disposent des processus et des ressources pour maintenir leurs activitÃ©s.

Dans le passÃ©, l'UE avait choisi dâ□□opter pour lâ□□entrÃ©e en vigueur de lÃ©gislations similaires en une seule fois, avec une date unique de mise en conformitÃ© ; comme ce fut le cas pour le RGPD.Â

Mais il serait judicieux d'apprendre des fonctions technologiques et informatiques de l'industrie. Il

faut en effet sâ□□assurer que l'objectif final est clair pour tous, en commenÃ§ant par un produit minimum viable ou une approche de type "pilote".

Il est ainsi prÃ©fÃ©rable de laisser le temps Ã tout le monde d'apprendre et de se familiariser avec la nouvelle rÃ©glementation, y compris le rÃ©gulateur lui-mÃªme, en commenÃ§ant par une catÃ©gorie de produit en particulier - telle que les ordinateurs et les tablettes - ou en examinant les exigences minimales si cela est viable.

Enfin, le rÃ¨glement final doit Ãªtre clair et trÃ¨s prÃ©cis quant aux responsabilitÃ©s qui incombent Ã chacun des acteurs.Â

En effet, la proposition actuelle indique : "Des obligations seront Ã©tablies pour les diffÃ©rents acteurs commerciaux, des fabricants aux distributeurs et importateurs, en ce qui concerne la mise sur le marchÃ© de produits contenant des Ã©lÃ©ments numÃ©riques, en fonction de leur rÃ´le et de leurs responsabilitÃ©s dans la supply chain" ; or, la majeure partie de ces objets connectÃ©s opÃ¨re dans des Ã©cosystÃ¨mes de R&D, de fabrication et de supply chain assez complexes.

De plus, le projet exige un "niveau de cybersÃ©curitÃ© appropriÃ©", ce qui ne semble pas suffisamment clair et concis pour ne pas engendrer de vides juridiques ou voir les parties prenantes se rejeter la faute Ã l'avenir quant Ã un manque de sÃ©curisation. Â»