Cyber Resilience Act : un enjeu majeur
Internet
PostÃ© par : JerryG
PubliÃ©e le : 11/12/2023 13:00:00

Le Parlement europÃ©en et le Conseil de l'Union europÃ©enne viennent de conclure un accord sur des rÃ¨gles visant Ã protÃ©ger les ordinateurs portables, les applications mobiles et les appareils intelligents connectÃ©s Ã Internet contre les cybermenaces, au travers du Cyber Resilience Act, dans un contexte d'attaques et de ransomwares qui se multiplient dans le monde entier ces derniÃ¨res annÃ©es.

DÃ¨s son entrÃ©e en vigueur en 2024, les fabricants, importateurs et distributeurs de matÃ©riel et de logiciels auront trois ans pour s'adapter aux exigences du rÃ¨glement.

Paolo Passeri, Cyber Intelligence Specialist chez Netskope, explique pourquoi ce rÃ¨glement est si important dans le contexte actuel et futur :

Â« La sÃ©curisation des appareils connectÃ©s est un projet de grande envergure, car lâ□□accÃ©lÃ©ration de leur adoption a rapidement dÃ©passÃ© leurs capacitÃ©s en matiÃ¨re de sÃ©curitÃ©. L'absence de sÃ©curitÃ© aux stades de la conception, du dÃ©veloppement et de la production, ainsi que l'absence de mises Ã jour et de correctifs, ont rendu ces appareils trÃ¨s vulnÃ©rables aux cyberattaques ciblÃ©es.

Les acteurs malveillants trouvent chaque jour de nouveaux moyens d'infiltrer les appareils connectÃ©s, et cette tendance continuera de sâ□□accÃ©lÃ©rer Ã mesure que lâ□□IoT consolide sa prÃ©sence dans les usages, Ã la fois professionnels et personnels.

Il est difficile de croire que ce secteur n'a pas eu Ã se conformer Ã une quelconque rÃ©glementation en matiÃ¨re de cybersÃ©curitÃ© jusqu'Ã prÃ©sent. Des normes de base pour sÃ©curiser tous les appareils connectÃ©s, ainsi que des procÃ©dures d'Ã©valuation de la conformitÃ© plus strictes pour les produits critiques, sont attendues depuis longtemps.

L'un des principaux problÃ¨mes de cybersÃ©curitÃ© auxquels nous sommes confrontÃ©s aujourd'hui concerne la chaÃ®ne d'approvisionnement. Dans le secteur du retail, par exemple, l'une des principales menaces pour les utilisateurs est l'attaque MageCart.

Ce type de cyberattaque peut permettre de voler les informations bancaires sensibles des acheteurs en ligne, lorsqu'une page de paiement est compromise par l'exploitation d'une vulnÃ©rabilitÃ© qui permet aux attaquants d'insÃ©rer un code malveillant capable de voler les dÃ©tails de la carte bancaire.

Ces risques devraient Ãªtre attÃ©nuÃ©s par la loi sur la cyber-rÃ©silience, car les solutions logicielles et matÃ©rielles devront se conformer Ã de multiples exigences de sÃ©curitÃ©, telles que la sÃ©curitÃ© dÃ¨s la conception, l'obligation de tester une solution de sÃ©curitÃ© avant de la mettre sur le marchÃ©, ou la divulgation de la dÃ©couverte de nouvelles vulnÃ©rabilitÃ©s.

Quel que soit le secteur, les organisations sont exposÃ©es Ã des vulnÃ©rabilitÃ©s dÃ¨s lors qu'elles utilisent des produits logiciels ou des appareils connectÃ©s, ce qui met en pÃ©ril l'ensemble de l'Ã©cosystÃ¨me, jusqu'aux consommateurs finaux.

La loi sur la cyber-rÃ©silience aura un coÃ»t de mise en conformitÃ©, mais elle rÃ©duira

considÃ©rablement le risque de cyberattaques en comblant de nombreuses lacunes, avec des logiciels et des dispositifs connectÃ©s mieux sÃ©curisÃ©s, et en responsabilisant les fabricants. Avec la multiplication des attaques ces derniers mois, la sÃ©curitÃ© de la supply chain doit Ãªtre une prioritÃ© pour les entreprises et les responsables de la sÃ©curitÃ©.

C'est pourquoi le Cyber Resilience Act doit Ãªtre considÃ©rÃ© comme une vÃ©ritable opportunitÃ© d'amÃ©liorer la cybersÃ©curitÃ© Ã partir de la base, dans un effort collectif Ã travers l'Europe, plutÃ´t que comme une nouvelle contrainte rÃ©glementaire. Â»