Les craintes concernant le Cyber Resilience Act de l'UE sont-elles justifiées ?

Le Cyber Resilience Act ne devrait pas être perçu comme une menace pour l'open-source européen car les législateurs de l'UE sont bien conscients de son poids économique : la dernière révision du texte vient d'ailleurs d'être saluée pour sa meilleure prise en compte de l'écosystème. Une tribune proposée par Thomas Segura, spécialiste cybersécurité de Gitguardian.

Temps de lecture : minute

---

12 février 2024

Le mercredi 19 juillet, le Parlement européen a voté en faveur d'un nouveau cadre juridique majeur en matière de cybersécurité : le Cyber Resilience Act (CRA). Selon le communiqué de presse publié après le vote : *« Le projet de loi sur la résilience cybernétique approuvé par la commission de l'industrie, de la recherche et de l'énergie vise à garantir que les produits dotés de fonctionnalités numériques, tels que les téléphones ou les jouets, sont sécurisés, résistants aux menaces cybernétiques et fournissent suffisamment d'informations sur leurs propriétés de sécurité. »*

Ce choix d'exemples, aussi banals qu'ils puissent paraître, souligne subtilement un débat crucial entourant le CRA : sa large portée d'application. Alors que certains peuvent remettre en question l'inclusion de tels objets courants, cela reflète l'approche globale de la loi en matière de cybersécurité.

L'introduction du CRA est opportune et vitale. Elle représente un effort

concerté pour renforcer la résilience des produits numériques face aux menaces cybernétiques, exigeant une collaboration internationale et une prévoyance stratégique. Cette initiative est une avancée significative pour renforcer la défense cybernétique de l'UE et affirmer sa souveraineté numérique.

Pour contextualiser, l'Agence de l'Union européenne pour la cybersécurité (ENISA) met en évidence une escalade préoccupante tant en termes de fréquence que de complexité des cyberattaques ciblant l'UE, comme le détaille leur rapport sur le paysage des menaces. L'administration publique, représentant environ 19 % de ces attaques, s'est révélée être le secteur le plus vulnérable en 2022 et 2023.

Décryptage du Cyber Resilience Act : comment fonctionnera-t-il ?

Son objectif principal est d'établir une base universelle de cybersécurité pour tous les produits dotés de composants numériques vendus dans l'UE. Cela englobe un large éventail d'articles, des logiciels et des appareils connectés au réseau aux objets contenant des systèmes informatiques intégrés. De manière significative, la loi ne fait pas de distinction entre les produits destinés aux consommateurs et ceux destinés aux entreprises.

Pour gérer cette diversité de produits, la loi propose une catégorisation en trois niveaux de sécurité : la catégorie par défaut, la catégorie "Classe I" critique et la catégorie "Classe II". Selon la Commission européenne, on estime qu'une majorité (environ 90 %) des produits relèveront de la "catégorie par défaut".

Sur la base de cette catégorisation des produits, le CRA introduit des niveaux différenciés d'évaluations de sécurité. Notamment, le "logiciel critique" exige une évaluation rigoureuse par des tiers. Cependant, la

portée de la catégorisation n'est pas toujours claire. Par exemple, les disques durs : bien qu'ils soient généralement classés dans la catégorie par défaut, une ambiguïté survient lorsque ces disques durs sont utilisés dans des centres de données cloud traitant des données sensibles. Cette zone grise souligne la nécessité de lignes directrices plus nuancées au sein de la loi.

Un aspect du CRA qui se distingue est son approche rigoureuse en matière de mise en application grâce à des sanctions financières substantielles. Les vendeurs opérant sur le marché unique de l'UE encourent des amendes pouvant atteindre 15 millions d'euros ou 2,5 % de leur chiffre d'affaires mondial en cas de non-conformité. Cette mesure reflète un changement de perspective, considérant la sécurité comme un aspect fondamental et non négociable du développement des produits, plutôt que comme une considération secondaire.

Cette importance accordée à la responsabilité financière est une stratégie de l'UE. En attribuant un coût tangible aux risques liés à la cybersécurité - des coûts que certaines entreprises étaient historiquement prêtes à absorber - le CRA vise à rééquilibrer l'équation risque-récompense en faveur de mesures de sécurité renforcées.

Cependant, cela soulève une autre question fondamentale : qui dans la chaîne d'approvisionnement doit assumer la responsabilité ? Ou dit autrement, qui supporte le risque ?

Qui supporte le risque? La position du CRA sur la responsabilité

Le CRA est sans équivoque quant à l'attribution de la responsabilité de la sécurité des produits numériques : elle incombe aux fabricants. Dans les cas où le fabricant et le producteur de logiciels sont les mêmes, cela est clair. Cependant, la loi entre dans des eaux troubles lorsqu'il s'agit de

logiciels open-source. Définir la propriété de la sécurité pour un code écrit par une personne et réutilisé par une autre présente un défi complexe.

Il est important de rappeler que l'open-source est un pilier du logiciel moderne. Il représente généralement de 70 % à 90 % du code des applications Web et cloud - la société de sécurité des applications Synopsys a constaté que 98 % des applications analysées avec son service incluaient des logiciels open-source, et que 75 % de la base de code moyenne provenait de projets open-source.

Cela souligne le défi important auquel sont confrontées presque toutes les entreprises commerciales pour mener les diligences nécessaires. Elles doivent s'assurer que tous les composants open-source ont été évalués de manière précise.

Réactions de la communauté open-source

La principale préoccupation vient directement de la communauté open-source elle-même. De nombreux projets open-source de premier plan expriment leur inquiétude car le Cybersecurity Act semble suggérer que la responsabilité de la conformité devrait incomber aux développeurs open-source. Cela implique que si un logiciel vendu commercialement sur le marché de l'UE intègre un composant open-source, ses créateurs pourraient être tenus responsables de sa sécurité.

Cette interprétation littérale pourrait potentiellement créer une situation insoutenable pour ceux qui contribuent aux projets open-source.

Cependant, il est important de noter que le CRA exempte spécifiquement les logiciels open-source développés ou fournis en dehors des activités commerciales. Le problème semble cependant résider dans la façon dont le CRA définit l'activité open-source. La loi semble être imprégnée de l'idée que la plupart des activités open-source découlent d'un "travail

bienveillant", une perspective largement considérée comme dépassée dans le contexte actuel.

Par exemple, les projets recevant des dons ou ayant des contributeurs d'entreprises ne seraient pas considérés comme un travail bienveillant et relèveraient de la compétence de la loi. Mais cette vision est loin de la réalité : les activités open-source et commerciales sont souvent entremêlées dans des profils d'exploitation hybrides complexes. De nombreuses entreprises open-source développent des produits open-source avec des licences permissives, tout en monétisant leur activité grâce à la vente de services de support et de fonctionnalités premium.

Inversement, il n'est pas rare que les géants de la technologie emploient des ingénieurs à temps plein travaillant exclusivement sur certains des plus grands projets open-source. Cela met en évidence un désalignement significatif entre les législateurs de l'UE et la communauté open-source. Les acteurs clés du domaine open-source, tels que OpenSSF et la Fondation Debian, ont critiqué les législateurs pour ne pas les avoir consultés lors de la rédaction de la loi.

L'avenir de l'open-source sous le CRA

Malgré les préoccupations prédominantes, il est peu probable que le Cyber Resilience Act signale la fin des logiciels open-source dans l'Union européenne. Il est vrai que les versions actuelles du CRA ne définissent pas explicitement sa portée. Cependant, cela n'exclut pas la possibilité de futures modifications.

Le bouleversement potentiel causé par l'obligation pour chaque producteur de logiciels d'examiner tous ses composants open-source est tout simplement trop vaste. Il est probable que les plus grandes entreprises de l'industrie du marché unique, toutes fortement dépendantes des logiciels, utiliseront leur pouvoir de lobbying

considérable pour influencer la loi en leur faveur lorsqu'elles reconnaîtront l'impact potentiellement catastrophique. Les enjeux sont trop élevés et le risque de nuire à l'avantage concurrentiel de l'Europe est énorme.

Même si ces efforts échouent, il pourrait bien y avoir des motifs de contester la loi en justice en raison des ambiguïtés présentes dans le texte. Par conséquent, nous pouvons nous attendre à ce que le langage de la loi soit affiné dans les mois à venir. Idéalement, cela se fera grâce à une collaboration étroite avec les principales organisations open-source.

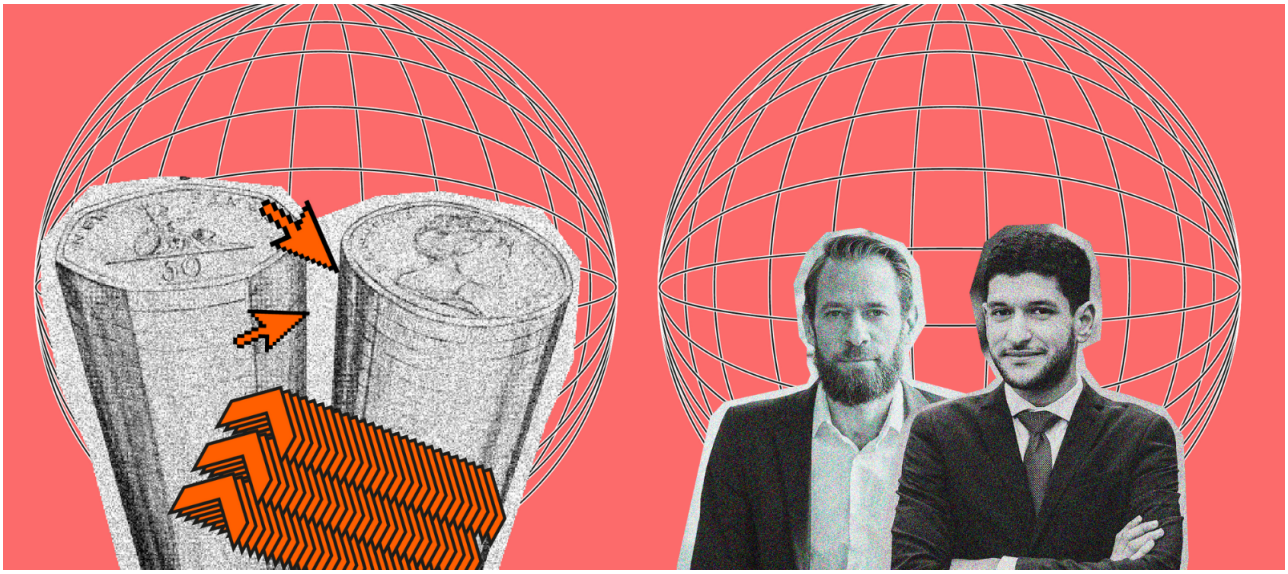
Une étape réglementaire avec des défis à relever

Le Cybersecurity Act représente une étape importante dans l'évolution réglementaire de l'Union européenne (UE), dans le but d'unifier les normes de cybersécurité sur son marché. Plus qu'une simple mesure réglementaire, le CRA est une déclaration politique, intentionnellement programmée pour démontrer l'engagement de l'UE dans la lutte contre les menaces cybernétiques. La portée large de la loi et son calendrier de mise en œuvre rapide peuvent être largement attribués aux turbulences géopolitiques actuelles.

Le CRA impose des mesures de sécurité tout au long du cycle de vie d'un produit, obligeant les fabricants à donner la priorité à la cybersécurité. Cette initiative audacieuse est essentielle pour renforcer la sécurité numérique au sein de l'UE. Cependant, la portée étendue de la loi et les nombreuses ambiguïtés qu'elle comporte ont également suscité des inquiétudes. Les craintes des organisations open-source de devoir assumer la responsabilité de la sécurité sont-elles justifiées ?

Bien qu'il revienne à chacun de se faire une opinion, il est possible que ces craintes ne soient pas entièrement justifiées, bien qu'il y ait une

certaine incertitude. L'existence de lacunes juridiques et les conséquences potentiellement importantes pour l'économie de l'UE si la loi est strictement appliquée dans son état actuel sont des arguments valables en faveur de futures améliorations. Ces améliorations devraient viser à renforcer, plutôt qu'à entraver, l'innovation et la résilience que la technologie open-source apporte au paysage numérique. Cependant, cela nécessitera de la vigilance.



À lire aussi
Cybersécurité : à quelles menaces faut-il s'attendre en 2024 ?

MADDYNEWS

Article écrit par Thomas Segura, spécialiste cybersécurité de Gitguardian