Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

Le CESIN analyse les implications du Cyber Resilience Act et renforce son engagement en faveur d'une cybersécurité robuste en Europe

Le Club des Experts de la Sécurité de l'Information et du Numérique accueille favorablement l'adoption du CRA par les co-législateurs européens, il souligne à la fois la nécessité d'une réglementation équilibrée, les points forts et défis à relever pour garantir la résilience du cyberespace européen.

Paris, le 20 mars 2024 – Le Cyber Resilience Act vise à améliorer la cybersécurité et la résilience des produits et services numériques en imposant des exigences de cybersécurité aux fabricants/éditeurs et détaillants. Ce règlement représente un jalon crucial dans la prise en compte des enjeux de sécurité du numérique au sein de l'Union européenne. L'association a suivi de près l'élaboration de ce règlement, contribuant activement à son avancement.

Cyber Resilience Act (CRA) : Des avancées et des préoccupations

La périodicité actuelle explicitée dans le Cyber Resilience Act offre aux acteurs du secteur le temps nécessaire pour adapter leurs pratiques et leurs infrastructures. Cette approche pragmatique favorise une transition fluide vers les nouvelles exigences réglementaires, en tenant compte des défis complexes auxquels le secteur est confronté. *« Nous saluons le calendrier raisonnable et la période de mise en œuvre cohérente établis par le CRA. Le CESIN, dans ses travaux auprès des co-législateurs, avait proposé une période de 21 à 24 mois pour la mise en conformité, en opposition à la période de 40 mois voulue par certains acteurs privés du secteur. »* se félicite **Mylène Jarossay, Présidente du CESIN.**

De même, le CESIN accueille favorablement la clarification et l'élargissement du champ d'application du CRA pour couvrir un large éventail de produits et services numériques sur le marché européen. Ainsi, le CRA introduit une clarté de périmètres et, par-là, une meilleure articulation avec la Directive NIS2 en ce qui concerne les exigences de cybersécurité relative au SaaS. Le CESIN est également rassuré de constater que les co-législateurs ont entendu la demande de responsabilité accrue de la part des éditeurs en ce qui concerne la sécurité des développements, qu'il s'agisse du service front assuré par le logiciel, mais aussi les fonctions backoffice d'administration et les services proposés pour les API. L'introduction de cette responsabilité accrue pour les éditeurs inclut aussi l'obligation de connaître et maîtriser tous les composants constituant son code, que ces composants soient écrits par l'éditeur en question ou utilisés par lui. Parmi les avancées positives, l'obligation pour l'éditeur de disposer, tenir à jour et mettre à disposition un inventaire précis des composants constituant son logiciel *(SBOM -*

Software Bill Of Materials). Le respect de cette disposition garantira une approche holistique de la cybersécurité dans le processus de développement.

Dans la continuité des exigences répondant aux défis contemporains, l'accent est mis sur le support et les correctifs tout au long du cycle de vie des produits et services numériques. Afin de veiller à la sécurité en continu, le CESIN salue cette approche astucieuse de distinguer les mises à jour introduisant des fonctionnalités de celles apportant des correctifs de sécurité. La nécessité pour les éditeurs de fournir ces correctifs de sécurité et de maintenir un historique des failles représente une avancée significative dans la transparence et la responsabilité en matière de cybersécurité. *« Ces dispositions reflètent nos recommandations et renforcent l'importance de garantir la sécurité dans tous les aspects du marché numérique européen. »* précise **Mylène Jarossay, Présidente du CESIN**

Cependant, malgré ces avancées, le CESIN reste préoccupé par certains aspects du CRA qui nécessitent une attention accrue. En particulier, l'association estime qu'une fréquence minimale d'audits de sécurité par un tiers indépendant devrait être clairement définie pour garantir une surveillance adéquate du marché. Dans ses recommandations émises pendant le processus d'élaboration du CRA, le CESIN proposait une fréquence minimale annuelle de ces audits, avec une communication transparente des problématiques identifiées et des mesures correctives prises.

Concernant le respect des obligations du CRA, le CESIN demande la nécessité d'une surveillance renforcée du marché et d'une coopération intersectorielle pour assurer une mise en œuvre efficace et cohérente du règlement. **Appelant à l'unité, le Club sollicite des mécanismes de coopération plus robustes entre les acteurs du marché et les autorités de contrôle**, **Mylène Jarossay**, déclare : *« Nous encourageons une représentation plus ouverte au sein de l'ADCO[1], permettant l'inclusion d'acteurs variés, universitaires, société civile, et secteur privé, pour une gouvernance équilibrée. Dans ce dispositif et avec la complexité croissante des compétences pluridisciplinaires à mobiliser, nous attirons l'attention vers l'identification de mécanismes de travail favorisant la bonne entente entre administrations et fonctions « métiers » et « technologie ».*

Le CESIN reste vigilant quant à l'étendue de responsabilités que le CRA donne à l'ENISA, l'Agence européenne de cybersécurité. Au-delà d'un rôle de soutien aux procédures d'enquête de la Commission européenne, le CRA devrait également établir un rôle explicite pour l'ENISA et la doter de moyens suffisants afin d'aider les autorités nationales dans leurs enquêtes, à leur propre demande, renforçant ainsi le suivi d'application au niveau technique. Tout comme dans le cadre des mécanismes de coopération intersectorielle, nous soulignons l'importance de renforcer les capacités opérationnelles de l'ENISA tout en évitant une bureaucratisation excessive des processus de surveillance et de réaction.

Rayna Stamboliyska, Présidente de RS Strategy, spécialiste des sujets de cyberdiplomatie et de résilience à travers les questions liées à la cybersécurité, a accompagné le CESIN sur cet axe,. Elle conclut : *« Restons unis dans notre engagement envers la sécurité du numérique dans toute l'Union européenne. Le CESIN continuera à oeuvrer activement pour promouvoir une cybersécurité robuste tout en garantissant une réglementation équilibrée et efficace. »*

1 ADCO : pour *ADministrative COoperation group*, est l'entité multipartite qui devra être établie pour veiller à l'application harmonisée du Règlement.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.
Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.
Le CESIN compte plus de 1 000 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

Pour en savoir plus www.cesin.fr