LES FICHES RÉGLEMENTAIRES CLOUD TEMPLE

Le Cyber Resilience Act, en clair

LES FAITS

Le Cyber Resilience Act (CRA), adopté en 2024, est un règlement européen qui impose des exigences de cybersécurité à tout produit matériel ou logiciel mis sur le marché européen, et ce, tout au long de son cycle de vie. Il introduit également une obligation de notification des vulnérabilités et renforce la transparence à l'égard des utilisateurs.

Il s'applique aux fabricants, importateurs et distributeurs de produits numériques mis sur le marché européen.

Le CRA entrera pleinement en application en 2027, avec une période de transition de 36 mois.

LE CONTEXTE

Le règlement CRA s'appuie sur la stratégie de cybersécurité de l'Union européenne adoptée en 2020, ainsi que sur la stratégie pour l'Union de la sécurité. Il complète d'autres instruments législatifs clés, en particulier la directive NIS2.

L'objectif du CRA est double : renforcer la protection des consommateurs et des entreprises face à la multiplication des incidents de cybersécurité, tout en harmonisant les exigences pour créer un marché intérieur plus sûr et plus compétitif.

POINTS CLÉS	CLARIFICATION
« Security by design » « Security by default »	Les produits numériques doivent être conçus avec des mesures de cybersécurité intégrées dès le départ (security by design) et des paramètres sécurisés activés par défaut (security by default).
Gestion des vulnérabilités	Les fabricants doivent mettre en place un processus de détection, correction et suivi des vulnérabilités, et publier des mises à jour de sécurité pendant toute la durée de vie du produit.
Transparence et information	Les utilisateurs doivent être informés des risques de cybersécurité, des bonnes pratiques, et de la durée pendant laquelle les mises à jour de sécurité seront assurées.
Conformité et surveillance	Le produit doit faire l'objet d'une évaluation de conformité (autodéclaration ou tierce partie), être accompagné d'une documentation technique, et respecter des obligations de notification en cas d'incident.

L'ANALYSE

Giuliano Ippoliti,
directeur cybersécurité de Cloud Temple

« Le Cyber Resilience Act marque une rupture majeure : la cybersécurité n'est plus une option, mais une propriété essentielle attendue dès la conception. En exigeant la maîtrise de chaque composant intégré, le texte touche au cœur du modèle cloud, fondé sur des chaînes logicielles interconnectées où la confiance repose sur la transparence. L'Europe envoie un signal fort : la cybersécurité devient un levier de compétitivité et de souveraineté technologique. »

OPEN SOURCE ET CYBER RESILIENCE

Bien que le CRA prévoie des exemptions pour les projets open source à but non lucratif et sans finalité commerciale, son application devient contraignante dès lors que des logiciels libres sont intégrés dans des produits ou services proposés dans un cadre économique.

Ces exigences incluent notamment la mise en place d'une documentation technique complète, la gestion proactive des vulnérabilités, la déclaration de conformité, l'apposition de marquage, ainsi que la fourniture d'une nomenclature logicielle.

Cela implique une transformation profonde des processus de développement, de suivi et de maintenance, avec un impact opérationnel et financier significatif.

CLOUD TEMPLE
Innovative by design