Guide pour comprendre le règlement sur la cyber-résilience

Barracuda

Il est essentiel que les organisations opérant au sein de l'Union européenne comprennent le règlement sur la cyber-résilience (Cyber Resilience Act ; CRA) de l'UE. Les fabricants de produits numériques commercialisés dans l'UE, ainsi que les importateurs et les distributeurs de ces produits, sont soumis au CRA. Cet e-book présente quelques grandes lignes du CRA à l'intention des fabricants concernés, mais il ne se substitue pas à des conseils juridiques et n'est pas destiné à constituer un avis juridique pour votre entreprise.

Entré en vigueur en décembre 2024, le CRA a accordé aux organisations un certain temps pour se mettre en conformité. Voici quelques dates clés à connaître :

- 11 septembre 2026 — Les fabricants doivent commencer à signaler les incidents graves de cybersécurité et les vulnérabilités activement exploitées.
- 11 décembre 2027 — Tous les produits entièrement nouveaux et les produits existants « substantiellement modifiés » mis sur le marché à cette date ou par la suite doivent se conformer au CRA.

Le règlement vise à uniformiser les exigences de sécurité pour tous les produits comportant des éléments numériques et commercialisés dans l'UE, et à fournir aux consommateurs et aux entreprises davantage d'informations sur leur sécurité avant de procéder à l'achat. Le CRA espère remédier à ce que l'UE qualifie de « niveau insuffisant » de la cybersécurité dans de nombreux produits, notamment en raison de l'absence de mises à jour de sécurité.

Le CRA complète le règlement sur la résilience opérationnelle numérique (DORA) et la directive sur la sécurité des réseaux et des informations 2 (NIS2) :

- Le règlement DORA se concentre sur l'amélioration de la cyber-résilience dans le secteur financier, et la directive NIS2 s'applique à un ensemble plus large d'entités fournissant des services essentiels dans des secteurs clés.
- DORA et NIS2 établissent tous deux des exigences en matière de cybersécurité, notamment des mesures de sécurité relatives à la chaîne logistique, dans le but d'accroître la résilience des entreprises réglementées, en raison de l'impact de leurs offres sur d'autres personnes.
- Le CRA s'applique au niveau du produit, en fournissant un cadre obligatoire afin de sécuriser les produits comportant des éléments numériques. Lorsque les clients achetant ces produits relèvent des réglementations DORA ou NIS2, l'utilisation de matériel et de logiciels conformes au CRA peut aider ces entités à respecter leurs obligations.

DORA et NIS2 ne sont pas abordés dans cet e-book. Veuillez consulter les e-books « Guide pour comprendre le règlement sur la résilience opérationnelle numérique (Digital Operational Resilience Act) » et « Appréhender la directive NIS2 : un guide sur les futures réglementations européennes en matière de cybersécurité » pour en savoir plus.

Pourquoi le CRA est-il important ?

Le CRA couvre tous les produits contenant des « éléments numériques », ce qui signifie qu'il concerne à la fois le matériel et le logiciel connecté à un appareil ou à un réseau, ainsi que les solutions intégrées de traitement des données à distance de ces produits (c'est-à-dire les services cloud). Selon la Commission européenne, « le règlement s'applique à tous les produits connectés directement ou indirectement à un autre appareil ou réseau, à l'exception de certaines exclusions spécifiques telles que certains logiciels open source ou produits de services qui sont déjà couverts par des règles en vigueur, ce qui est le cas des appareils médicaux, de l'aviation et des voitures ».[1] La commercialisation des produits non conformes ne sera pas autorisée dans l'UE. Les organisations prises en faute feront l'objet de sanctions financières. Tout comme le règlement général sur la protection des données (RGPD) a fondamentalement changé la manière dont les entreprises traitent les informations à caractère personnel, le CRA pourrait fortement influencer la façon dont les fabricants manufacturent, vendent et soutiennent leurs produits comportant des éléments numériques sur le marché de l'UE.

Le CRA s'attaque au problème croissant des produits technologiques modernes qui collectent, traitent, partagent et stockent les données des utilisateurs, souvent dans un cadre de sécurité faible ou inexistant, ce qui fait courir un grand danger à ces données. À mesure que ces produits vieillissent, les solutions de sécurité disponibles peuvent devenir obsolètes. Il existe peu de contrôles concernant la manière dont les mises à jour de sécurité sont fournies aux utilisateurs, quand elles le sont, voire même si elles le sont. Le CRA cherche à accroître la sécurité des produits comportant des éléments numériques et à s'assurer que ces produits restent sécurisés tout au long de leur cycle de vie. Ce règlement apportera également une plus grande transparence aux utilisateurs, qui auront une meilleure compréhension de la sécurité des produits contenant des éléments numériques et de la manière dont cela pourrait affecter leurs données.

[1] Règlement sur la cyber-résilience | Façonner l'avenir numérique de l'Europe

Obligations des fabricants dans le cadre du CRA

Le CRA introduit des exigences obligatoires en matière de cybersécurité pour les fabricants ; ces exigences régissent la planification, la conception, le développement, la production, la livraison, la documentation et la maintenance des produits concernés. Ces obligations doivent être respectées à chaque étape de la chaîne de valeur.

En vertu du CRA, les produits peuvent être classés comme standard dans la catégorie « par défaut » (niveau le plus bas), comme « importants » (assortis de plus d'obligations) — cette catégorie étant divisée en deux sous-catégories, la classe I et la classe II — et comme « critiques » (dotés du niveau de risque le plus élevé et donc assortis des obligations les plus strictes).

Pour les articles standard, les fabricants sont tenus de concevoir, de fabriquer et de tester les biens et services afin de vérifier leur conformité aux « exigences essentielles de cybersécurité » spécifiées à l'Annexe I du CRA, de documenter l'évaluation et de tenir la documentation technique à la disposition des autorités de surveillance du marché. À ce niveau, les fabricants peuvent s'appuyer sur une évaluation de conformité interne (auto-évaluation).

De manière générale, environ 90 % des produits matériels et logiciels devraient appartenir à cette catégorie « par défaut », qui permet aux fabricants de s'auto-évaluer et de créer une déclaration de conformité avant d'apposer le marquage CE correspondant aux produits conformes.

Certains produits comportant des éléments numériques, tels que les navigateurs Web, les pare-feux et les systèmes d'exploitation, entrent dans la catégorie des produits « importants » ; d'autres relèvent même de la catégorie « critiques ». Ils doivent toujours respecter les exigences techniques de l'Annexe I mais peuvent être soumis à un processus d'évaluation de la conformité plus strict, notamment une évaluation/certification tierce, avant d'être commercialisés dans l'UE.

Outre les obligations au moment de la vente, le CRA exige également que les fabricants fournissent une gestion des vulnérabilités et des correctifs de sécurité, comme décrit ci-dessous.

Obligations de signalement de sécurité

Le signalement des vulnérabilités de sécurité activement exploitées et des incidents graves dans le cadre du CRA deviendra obligatoire le 11 septembre 2026.

Les obligations de signalement sont strictes. Les fabricants devront notifier une « alerte précoce » aux autorités compétentes au plus tard 24 heures après avoir eu connaissance du problème. Au plus tard 72 heures après avoir eu connaissance d'une vulnérabilité exploitée, les fabricants devront fournir des informations générales sur le produit concerné, une description générale de la vulnérabilité exploitée, décrire toute action d'atténuation entreprise par le fabricant et que les utilisateurs peuvent entreprendre, et indiquer le niveau de sensibilité du problème. Dans les 14 jours suivant la mise à disposition des mesures d'atténuation, le fabricant a d'autres obligations de divulgation sous la forme d'un rapport final.

Les obligations de signalement comprennent également l'information des utilisateurs concernés et la fourniture de conseils concernant les moyens d'atténuer leur exposition.

Les fabricants devraient se familiariser avec ces exigences en matière de signalement et mettre au point des processus pour s'y conformer d'ici leur date d'entrée en vigueur en septembre 2026.

Obligations de support technique

L'assistance en matière de cybersécurité, plus précisément la fourniture de mises à jour de sécurité, est également un sujet important pour le CRA ; elle doit être planifiée de manière à couvrir l'ensemble du cycle de vie du produit. Les fabricants doivent spécifier à l'avance la période d'assistance pour les produits comportant des éléments numériques. En général, les entreprises qui commercialisent des produits contenant des éléments numériques dans l'UE doivent fournir une assistance pendant au moins cinq ans, sauf si la durée de vie prévue du produit est inférieure — dans ce cas, l'assistance doit couvrir toute la durée de vie prévue du produit. Pour les produits dont la durée de vie est généralement supérieure à cinq ans (p. ex., cartes mères, routeurs réseau, modems, commutateurs et systèmes d'exploitation), la période d'assistance devrait être plus longue. Les mises à jour de sécurité doivent être à la disposition des utilisateurs pendant toute la période d'assistance ou pendant au moins dix ans, la période la plus longue étant retenue.

Comment la conformité sera-t-elle appliquée ?

La non-conformité peut entraîner des pénalités, tant financières — amendes allant jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires mondial total — que non financières. Les autorités réglementaires pourraient contraindre une entreprise à rappeler les produits non conformes.

Barracuda

Six étapes de conformité pour les fabricants

Vous trouverez ci-dessous les étapes de base que les fabricants doivent suivre pour entamer leur processus de conformité, afin d'être prêts à répondre aux exigences du CRA lorsqu'il entrera pleinement en vigueur. Les multiples annexes du CRA fournissent des détails sur ce qui est attendu à chaque étape.

1. Classez les produits et effectuez une évaluation des risques cyber. Les organisations peuvent avoir des produits dans plusieurs catégories. Il est donc important d'évaluer chaque produit pour déterminer sa catégorie : Par défaut (standard), Important ou Critique.

2. Préparez la documentation technique. Étudiez l'Annexe I du CRA et les exigences relatives à la chaîne logistique pour tous les produits, et identifiez les éventuelles lacunes. Réalisez et documentez une évaluation des risques pour chaque produit par rapport aux critères applicables et aux normes pertinentes identifiées, aux spécifications communes ou aux systèmes de certification appropriés.

3. Déterminez l'approche d'évaluation de la conformité pour chaque produit. Si nécessaire, faites appel à un tiers pour cet exercice.

4. Préparez une déclaration de conformité conformément à l'Annexe V/VI et complétez la documentation technique visée à l'Annexe VII. Le fabricant doit ensuite apposer le marquage CE sur le produit conforme, son emballage ou sa documentation. Le marquage CE indiquera la conformité des produits comportant des éléments numériques avec le CRA, afin qu'ils puissent circuler librement au sein de l'UE.

5. Préparez et fournissez les informations/instructions utilisateur conformément à l'Annexe II. La documentation est un élément essentiel de la conformité et de son objectif de transparence vis-à-vis de l'utilisateur.

6. Surveillez et gérez les vulnérabilités. Le CRA exige une participation active et continue des fabricants pendant la période de la couverture d'assistance, qui comprend l'accès à une assistance de cybersécurité, la surveillance des vulnérabilités ainsi que le signalement et la correction des lacunes, par exemple au moyen de mises à jour logicielles visant à résoudre les problèmes de sécurité.

Barracuda s'emploie activement à confirmer les catégories de ses produits et à se préparer aux étapes suivantes. Nous vous fournirons des informations sur notre Trust Center dès qu'elles seront disponibles.

ÉTAPE 1
Classez les produits et réalisez une analyse des risques cyber pour chaque produit

ÉTAPE 2
Préparez la documentation technique

ÉTAPE 3
Déterminez l'approche d'évaluation de la conformité

ÉTAPE 4
Appliquez le marquage CE et rédigez une déclaration de conformité

ÉTAPE 5
Préparez et fournissez des instructions utilisateur

ÉTAPE 6
Surveillez et gérez les vulnérabilités

Produits importants de classe I et II

Les produits importants de classe I présentent des risques en matière de cybersécurité qui sont inférieurs à ceux des produits importants de classe II. Les fabricants peuvent choisir d'autodéclarer la conformité s'ils satisfont à certaines exigences en matière de normes/spécifications communes/systèmes de certification qualifiés de l'UE, à condition qu'ils soient disponibles et applicables au produit. Sinon, il est possible qu'une vérification par un tiers soit requise.

Les produits importants de classe II sont considérés comme présentant des risques plus élevés en matière de cybersécurité, et une certification par un tiers autorisé est requise.

Collectivement, les réglementations CRA, DORA et NIS2 forment un ensemble complexe de règles en matière de cybersécurité pour les entreprises opérant dans l'UE. Votre entreprise peut être soumise à plusieurs de ces réglementations. Le Trust Center de Barracuda contient diverses ressources pour aider les clients à comprendre DORA, notamment notre e-book « Guide pour comprendre le règlement sur la résilience opérationnelle numérique (Digital Operational Resilience Act) », et NIS2, notamment notre e-book « Appréhender la directive NIS2 : un guide sur les futures réglementations européennes en matière de cybersécurité », afin d'aider les entreprises à respecter leurs obligations de conformité.

Barracuda

Barracuda en quelques mots

Barracuda est une entreprise mondiale de cybersécurité de premier plan qui fournit une protection complète contre les menaces complexes aux entreprises de toutes tailles. Notre plateforme BarracudaONE alimentée par l'IA protège les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes, à une plateforme XDR gérée et à un tableau de bord centralisé afin de maximiser la protection et de renforcer la cyber-résilience. Forte de la confiance de centaines de milliers de professionnels de l'informatique et de fournisseurs de services gérés dans le monde entier, Barracuda propose des défenses puissantes, faciles à acheter, à déployer et à utiliser. Pour plus d'informations, visitez fr.barracuda.com.

Barracuda