SE

EMBEDDED SYSTEMS ENGINEERING

SCHMITT CONSULTING S.A.R.L. · SC-SARL.COM

Check rapide CRA pour fabricants d'appareils

La nouvelle loi européenne sur la cybersécurité des produits connectés — ce qui doit être en place d'ici septembre 2026, en langage clair.

Première échéance contraignante : 11 septembre 2026

Pas 2027. Qui ne se prépare pas dès maintenant manquera de temps.

1 De quoi il s'agit

Le **Cyber Resilience Act** — en abrégé **CRA** — est en vigueur depuis décembre 2024. Il prescrit le niveau de sécurité que les produits connectés doivent atteindre face aux attaques venues d'Internet. Sont concernés tous les produits qui contiennent un logiciel ou se connectent à un réseau : du thermostat intelligent aux automates industriels en passant par l'application.

Beaucoup de fabricants pensent avoir jusqu'à fin 2027. Cela n'est vrai que pour une partie des obligations. La **première échéance contraignante tombe dès septembre 2026** — et elle concerne aussi les produits déjà sur le marché et encore maintenus.

11 septembre 2026

Obligation de signalement. Si une faille de sécurité est manifestement exploitée par des attaquants, elle doit être signalée aux autorités **dans les 24 heures**.

11 décembre 2027

Toutes les autres obligations. Produit sûr dès la conception, mises à jour de sécurité sur toute la durée de vie, nomenclature logicielle complète, évaluation formelle et marquage CE.

Les amendes possibles atteignent **15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial** — le montant le plus élevé étant retenu. Et : la loi s'applique expressément aussi aux petits fabricants et aux indépendants, pas seulement aux grands groupes.

2 Les notions clés — en bref

Firmware
Le logiciel de commande intégré de façon permanente à un appareil et qui le fait fonctionner — par exemple le code programme d'une machine, d'un capteur ou d'un automate.

Faille de sécurité (vulnérabilité)
Un défaut ou une faiblesse du logiciel par lequel un attaquant peut s'introduire dans l'appareil ou le manipuler.

Nomenclature logicielle (SBOM)
Une liste complète de tous les composants logiciels d'un produit — comparable à la nomenclature d'un composant, mais pour le code programme. Sans elle, impossible de dire si le produit est touché par une faille connue.

ENISA / CSIRT
L'ENISA est l'agence européenne de cybersécurité, l'organe central de la sécurité informatique en Europe. Les CSIRT sont les « pompiers informatiques » nationaux qui coordonnent en cas d'incident. C'est à eux que va le signalement sous 24 heures.

Sécurité fonctionnelle
La protection d'un appareil contre les *dysfonctionnements et défaillances* techniques — pratique établie notamment dans l'automobile. Le CRA y ajoute la protection contre les *attaques délibérées*.

Marquage CE
Le marquage CE bien connu sur les produits. Il atteste qu'un produit respecte les exigences de l'UE et peut être vendu sur le marché européen.

3 Êtes-vous prêt pour le CRA ? La liste de contrôle

Parcourez les points suivants. Chaque case que vous **ne pouvez pas** cocher en toute bonne conscience est un chantier ouvert jusqu'à septembre 2026.

VUE D'ENSEMBLE & ORGANISATION

- ☐ Nous savons lesquels de nos produits relèvent de la loi.
- ☐ Nous savons quels produits plus anciens nous maintenons encore (et qui sont donc également concernés).
- ☐ Une personne est responsable du sujet CRA dans l'entreprise.

NOMENCLATURE LOGICIELLE

- ☐ Pour chaque produit, il existe une liste complète de tous les composants logiciels intégrés.
- ☐ Nous y repérons aussi les composants obsolètes que le fournisseur ne maintient plus.
- ☐ Cette liste est tenue à jour en continu, et non établie une seule fois.

PROCESSUS DE SIGNALEMENT (OBLIGATOIRE DÈS 09/2026)

- ☐ Il est défini qui détecte une faille exploitée.
- ☐ Il est défini qui l'évalue et qui la signale.
- ☐ Nous pouvons réellement respecter le délai de 24 heures sur le plan organisationnel — y compris le week-end.

PROTECTION TECHNIQUE DE L'APPAREIL

- ☐ Le logiciel de l'appareil est stocké chiffré et ne peut pas être simplement lu.
- ☐ Les mises à jour sont infalsifiables — personne ne peut injecter un logiciel frauduleux.
- ☐ L'appareil peut recevoir des mises à jour de sécurité durant toute sa durée de vie.
- ☐ Au démarrage, l'appareil vérifie que seul un logiciel authentique et non modifié s'exécute.

PREUVES & DOCUMENTATION

- ☐ Nous pouvons prouver que le développement a suivi des normes de programmation reconnues.
- ☐ Sûreté de fonctionnement et résistance aux attaques sont pensées dans un concept commun, non séparé.
- ☐ Les documents nécessaires à l'évaluation de conformité ultérieure sont tenus dès le départ.

4 La suite

Les prochains mois décideront si, en septembre 2026, un processus ordonné est en place ou s'il faudra improviser dans la précipitation. Qui commence tôt répartit le travail — et évite des corrections coûteuses juste avant l'échéance. Le levier le plus important ne réside généralement pas dans la seule technique, mais dans la bonne articulation entre nomenclature, processus de signalement et protection de l'appareil.

→ Aller plus loin & accompagnement

Vous ne voulez pas seulement comprendre les exigences, mais les mettre en œuvre ? Trois voies :

Ouvrages techniques & logiciels

Un savoir issu de plus de 35 ans de développement embarqué — la base technique derrière les exigences du CRA. À découvrir sur **sc-sarl.com/fr/produkte.html**

Offert : « Recueil de formules pour informaticiens et ingénieurs »

Recueil de formules HTML interactif, 56 chapitres, bilingue DE/EN, utilisable hors ligne — gratuit dans l'espace de téléchargement.

Accompagnement personnalisé

De la nomenclature logicielle au durcissement du firmware. Entretien-conseil sur **sc-sarl.com/fr/kontakt.html**

Vers les produits & téléchargements →

Ce guide donne un aperçu pratique et ne remplace pas un conseil juridique. Le texte de référence est le règlement (UE) 2024/2847. État des échéances : obligation de signalement à partir du 11/09/2026, pleine applicabilité à partir du 11/12/2027.