SE

EMBEDDED SYSTEMS ENGINEERING

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

Бърза проверка CRA за производители на устройства

Новият закон на ЕС за киберсигурността на свързаните продукти — какво трябва да е готово до септември 2026 г., на разбираем език.

Първи задължителен срок: 11 септември 2026 г.

Не чак 2027. Който не се подготви сега, ще изпадне в недостиг на време.

1 За какво става дума

Cyber Resilience Act — накратко **CRA** — е в сила от декември 2024 г. Той определя колко сигурни трябва да са свързаните продукти срещу атаки от интернет. Засяга всичко, което съдържа софтуер или се свързва към мрежа: от интелигентния термостат през промишлените контролери до приложението.

Много производители смятат, че имат време до края на 2027 г. Това важи само за част от задълженията. **Първият задължителен срок е още през септември 2026 г.** — и засяга и продукти, които отдавна са на пазара и все още се поддържат.

11 септември 2026 г.

Задължение за уведомяване. Ако уязвимост бъде доказуемо използвана от нападатели, това трябва да се съобщи на органите **в рамките на 24 часа**.

11 декември 2027 г.

Всички останали задължения. Продукт, сигурен по замисъл, актуализации на сигурността през целия жизнен цикъл, пълен списък на софтуерните компоненти, формална оценка и маркировка CE.

Възможните глоби достигат до **15 милиона евро или 2,5 % от световния годишен оборот** — в зависимост от това коя сума е по-висока. И: законът се прилага изрично и за малки производители и единични доставчици, не само за големите концерни.

2 Най-важните понятия — накратко

Фърмуер (firmware)
Управляващият софтуер, трайно вграден в устройството, който изобщо го кара да работи — например програмният код в машина, сензор или контролер.

Уязвимост (пробив в сигурността)
Грешка или слабост в софтуера, чрез която нападател може да проникне в устройството или да го манипулира.

Списък на софтуерните компоненти (SBOM)
Пълен списък на всички софтуерни компоненти на продукта — сравним със спецификацията на детайл, но за програмния код. Без него не може да се каже дали продуктът е засегнат от известна уязвимост.

ENISA / CSIRT
ENISA е агенцията на ЕС за киберсигурност, централният орган за ИТ сигурност в Европа. CSIRT са националните държавни «компютърни пожарни», които координират при инциденти със сигурността. До тях отива уведомлението в рамките на 24 часа.

Функционална безопасност
Защитата на устройство срещу технически *неизправности и откази* — утвърдена практика например в автомобилната техника. CRA я допълва със защита срещу *преднамерени атаки*.

Маркировка CE
Известната маркировка CE върху продуктите. Тя потвърждава, че продуктът отговаря на изискванията на ЕС и може да се продава на европейския пазар.

3 Готови ли сте за CRA? Контролният списък

Прегледайте следните точки. Всяко квадратче, което **не** можете със спокойна съвест да отметнете, е отворен фронт до септември 2026 г.

ПРЕГЛЕД И ОРГАНИЗАЦИЯ

- ☐ Знаем кои от продуктите ни попадат под закона.
- ☐ Знаем кои по-стари продукти все още поддържаме (и които следователно също са засегнати).
- ☐ Във фирмата има отговорно лице по темата CRA.

СПИСЪК НА СОФТУЕРНИТЕ КОМПОНЕНТИ

- ☐ За всеки продукт съществува пълен списък на всички вградени софтуерни компоненти.
- ☐ В него разпознаваме и остарелите компоненти, които доставчикът вече не поддържа.
- ☐ Този списък се поддържа постоянно актуален, а не се изготвя еднократно.

ПРОЦЕС НА УВЕДОМЯВАНЕ (ЗАДЪЛЖИТЕЛЕН ОТ 09/2026)

- ☐ Определено е кой забелязва използвана уязвимост.
- ☐ Определено е кой я оценява и кой я докладва.
- ☐ Можем организационно действително да спазим 24-часовия срок — и през уикенда.

ТЕХНИЧЕСКА ЗАЩИТА НА УСТРОЙСТВОТО

- ☐ Софтуерът в устройството се съхранява шифрован и не може просто да се прочете.
- ☐ Актуализациите са защитени от подправяне — никой не може да внедри подхвърлен софтуер.
- ☐ Устройството може да получава актуализации на сигурността през целия си жизнен цикъл.
- ☐ При стартиране устройството проверява, че се изпълнява само автентичен, непроменен софтуер.

ДОКАЗАТЕЛСТВА И ДОКУМЕНТАЦИЯ

- ☐ Можем да докажем, че разработката е следвала признати стандарти за програмиране.
- ☐ Надеждността и устойчивостта на атаки са замислени в една обща концепция, не поотделно.
- ☐ Документите, необходими за по-късната оценка на съответствието, се водят от самото начало.

4 Как се продължава

Следващите месеци ще решат дали през септември 2026 г. ще има подреден ход или ще трябва да се импровизира припряно. Който започне рано, разпределя работата — и избягва скъпи аварийни решения непосредствено преди срока. Най-голямата лост обикновено не е само в техниката, а в чистото взаимодействие между списъка, процеса на уведомяване и защитата на устройството.

→ По-задълбочено и подкрепа

Не искате само да обхванете изискванията, а да ги приложите? Три пътя:

Специализирани книги и софтуер

Практически знания от над 35 години вградена разработка — техническата основа зад изискванията на CRA. Намира се на **sc-sarl.com/bg/produkte.html**

Безплатно към това: «Сборник с формули за информатици и инженери»

Интерактивен HTML сборник с формули, 56 глави, двуезичен DE/EN, използваем офлайн — безплатно в зоната за изтегляне.

Лична подкрепа

От списъка на софтуерните компоненти до закаляването на фърмуера. Консултация на **sc-sarl.com/bg/kontakt.html**

Към продуктите и изтеглянията →