SE

EMBEDDED SYSTEMS ENGINEERING

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

Szybki test CRA dla producentów urządzeń

Nowe unijne prawo o cyberbezpieczeństwie produktów połączonych z siecią — co musi być gotowe do września 2026, zrozumiałym językiem.

Pierwszy wiążący termin: 11 września 2026

Nie dopiero w 2027. Kto nie przygotuje się teraz, znajdzie się pod presją czasu.

1 O co chodzi

Cyber Resilience Act — w skrócie **CRA** — obowiązuje od grudnia 2024 r. Określa, jak bezpieczne muszą być produkty połączone z siecią wobec ataków z internetu. Dotyczy wszystkiego, co zawiera oprogramowanie lub łączy się z siecią: od inteligentnego termostatu przez sterowniki przemysłowe po aplikację.

Wielu producentów sądzi, że mają czas do końca 2027 r. Dotyczy to tylko części obowiązków. **Pierwszy wiążący termin przypada już we wrześniu 2026 r.** — i obejmuje także produkty od dawna obecne na rynku i nadal wspierane.

11 września 2026

Obowiązek zgłaszania. Jeśli luka jest w sposób udowodniony wykorzystywana przez atakujących, należy zgłosić to organom **w ciągu 24 godzin**.

11 grudnia 2027

Wszystkie pozostałe obowiązki. Produkt bezpieczny od podstaw, aktualizacje zabezpieczeń przez cały okres eksploatacji, pełny wykaz składników oprogramowania, formalna ocena i oznakowanie CE.

Możliwe kary sięgają **15 milionów euro lub 2,5 % światowego rocznego obrotu** — w zależności od tego, która kwota jest wyższa. Oraz: prawo wyraźnie dotyczy także małych producentów i pojedynczych dostawców, nie tylko wielkich koncernów.

2 Najważniejsze pojęcia — w skrócie

Oprogramowanie układowe (firmware)

Oprogramowanie sterujące wbudowane na stałe w urządzenie, które sprawia, że w ogóle działa — na przykład kod programu w maszynie, czujniku lub sterowniku.

Luka (podatność)

Błąd lub słabość oprogramowania, przez którą atakujący może wniknąć do urządzenia lub nim manipulować.

Wykaz składników oprogramowania (SBOM)

Kompletna lista wszystkich składników oprogramowania produktu — porównywalna z listą części podzespołu, lecz dla kodu programu. Bez niej nie da się stwierdzić, czy produkt dotyka znana luka.

ENISA / CSIRT

ENISA to unijna agencja ds. cyberbezpieczeństwa, centralny organ bezpieczeństwa IT w Europie. CSIRT to krajowe państwowe «straże pożarne dla komputerów», które koordynują działania przy incydentach. To do nich trafia zgłoszenie w ciągu 24 godzin.

Bezpieczeństwo funkcjonalne

Ochrona urządzenia przed technicznymi *usterkami i awariami* — utrwalona praktyka m.in. w technice motoryzacyjnej. CRA uzupełnia ją o ochronę przed *celowymi atakami*.

Oznakowanie CE

Znane oznakowanie CE na produktach. Potwierdza, że produkt spełnia wymogi UE i może być sprzedawany na rynku europejskim.

3 Czy jesteś gotów na CRA? Lista kontrolna

Przejdź przez poniższe punkty. Każde okienko, którego **nie** możesz z czystym sumieniem zaznaczyć, to otwarta sprawa do września 2026 r.

PRZEGLĄD I ORGANIZACJA

- ☐ Wiemy, które z naszych produktów podlegają temu prawu.
- ☐ Wiemy, które starsze produkty nadal wspieramy (i które są tym samym także objęte).
- ☐ W firmie jest osoba odpowiedzialna za temat CRA.

WYKAZ SKŁADNIKÓW OPROGRAMOWANIA

- ☐ Dla każdego produktu istnieje kompletna lista wszystkich wbudowanych składników oprogramowania.
- ☐ Rozpoznajemy w niej także przestarzałe elementy, których dostawca już nie wspiera.
- ☐ Lista ta jest na bieżąco aktualizowana, a nie tworzona jednorazowo.

PROCES ZGŁASZANIA (OBOWIĄZKOWY OD 09/2026)

- ☐ Ustalono, kto zauważa wykorzystaną lukę.
- ☐ Ustalono, kto ją ocenia i kto ją zgłasza.
- ☐ Potrafimy organizacyjnie rzeczywiście dotrzymać terminu 24 godzin — także w weekend.

TECHNICZNE ZABEZPIECZENIE URZĄDZENIA

- ☐ Oprogramowanie w urządzeniu jest zapisane w postaci zaszyfrowanej i nie da się go po prostu odczytać.
- ☐ Aktualizacje są zabezpieczone przed sfałszowaniem — nikt nie może wgrać podstawionego oprogramowania.
- ☐ Urządzenie może otrzymywać aktualizacje zabezpieczeń przez cały okres eksploatacji.
- ☐ Przy starcie urządzenie sprawdza, że działa tylko autentyczne, niezmienione oprogramowanie.

DOWODY I DOKUMENTACJA

- ☐ Potrafimy wykazać, że rozwój przebiegał według uznanych standardów programowania.
- ☐ Niezawodność i odporność na ataki są ujęte w jednej wspólnej koncepcji, a nie oddzielnie.
- ☐ Dokumenty potrzebne do późniejszej oceny zgodności prowadzone są od samego początku.

4 Co dalej

Najbliższe miesiące zdecydują, czy we wrześniu 2026 r. będzie uporządkowany przebieg, czy trzeba będzie pospiesznie improwizować. Kto zacznie wcześnie, rozłoży pracę — i uniknie kosztownych prowizorek tuż przed terminem. Największa dźwignia zwykle nie tkwi w samej technice, lecz w sprawnym współgraniu wykazu, procesu zgłaszania i zabezpieczenia urządzenia.

→ Głębiej i wsparcie

Nie chcesz tylko ogarnąć wymagań, ale je wdrożyć? Trzy drogi:

Książki fachowe i oprogramowanie

Wiedza praktyczna z ponad 35 lat rozwoju systemów wbudowanych — techniczna podstawa stojąca za wymaganiami CRA. Do znalezienia na **sc-sarl.com/pl/produkte.html**

Gratis do tego: «Zbiór wzorów dla informatyków i inżynierów»

Interaktywny zbiór wzorów w HTML, 56 rozdziałów, dwujęzyczny DE/EN, działa offline — bezpłatnie w sekcji pobierania.

Wsparcie indywidualne

Od wykazu składników oprogramowania po utwardzanie firmware'u. Rozmowa doradcza na **sc-sarl.com/pl/kontakt.html**

Do produktów i pobrań →