SE

EMBEDDED SYSTEMS ENGINEERING

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

CRA gyorsellenőrzés eszközgyártóknak

Az EU új törvénye a hálózatba kötött termékek kiberbiztonságáról — minek kell készen állnia 2026 szeptemberéig, érthető nyelven.

Első kötelező határidő: 2026. szeptember 11.

Nem csak 2027-ben. Aki most nem készül fel, időzavarba kerül.

1 Miről van szó

A **Cyber Resilience Act** — röviden **CRA** — 2024 decembere óta hatályos. Előírja, mennyire biztonságosnak kell lenniük a hálózatba kötött termékeknek az internetről érkező támadásokkal szemben. Mindenre kiterjed, ami szoftvert tartalmaz vagy hálózatra csatlakozik: az okostermosztáttól az ipari vezérlőkön át az alkalmazásig.

Sok gyártó azt hiszi, hogy 2027 végéig van ideje. Ez csak a kötelezettségek egy részére igaz. Az **első kötelező határidő már 2026 szeptemberében esedékes** — és kiterjed a régóta piacon lévő, még karbantartott termékekre is.

2026. szeptember 11.

Bejelentési kötelezettség. Ha egy sebezhetőséget támadók bizonyíthatóan kihasználnak, azt **24 órán belül** jelenteni kell a hatóságoknak.

2027. december 11.

Az összes többi kötelezettség. Alapjaiban biztonságos termék, biztonsági frissítések a teljes élettartam alatt, teljes szoftverösszetétel-jegyzék, formális értékelés és CE-jelölés.

A lehetséges bírságok elérik a **15 millió eurót vagy a globális éves árbevétel 2,5 %-át** — attól függően, melyik összeg a magasabb. És: a törvény kifejezetten a kis gyártókra és egyéni beszállítókra is vonatkozik, nem csak a nagy konszernekre.

2 A legfontosabb fogalmak — röviden

Firmware (vezérlőszoftver)

Az eszközbe tartósan beépített vezérlőszoftver, amely egyáltalán működésre bírja — például egy gép, érzékelő vagy vezérlő programkódja.

Sebezhetőség (biztonsági rés)

A szoftver olyan hibája vagy gyengesége, amelyen keresztül egy támadó behatolhat az eszközbe vagy manipulálhatja azt.

Szoftverösszetétel-jegyzék (SBOM)

Egy termék összes szoftverösszetevőjének teljes listája — egy alkatrész darabjegyzékéhez hasonló, de a programkódhoz. Nélküle nem mondható meg, érinti-e a terméket egy ismert sebezhetőség.

ENISA / CSIRT

Az ENISA az EU kiberbiztonsági ügynöksége, az európai IT-biztonság központi szerve. A CSIRT-ek a nemzeti állami «számítógépes tűzoltóságok», amelyek biztonsági incidensek esetén koordinálnak. Hozzájuk megy a 24 órás bejelentés.

Funkcionális biztonság

Egy eszköz védelme a műszaki *meghibásodásokkal és kiesésekkel* szemben — bevett gyakorlat például a járműtechnikában. A CRA ezt kiegészíti a *szándékos támadások* elleni védelemmel.

CE-jelölés

A jól ismert CE-jelölés a termékeken. Megerősíti, hogy a termék megfelel az EU követelményeinek, és értékesíthető az európai piacon.

3 Felkészültek a CRA-ra? Az ellenőrzőlista

Menjenek végig a következő pontokon. Minden négyzet, amelyet **nem** tudnak nyugodt lelkiismerettel kipipálni, nyitott építkezés 2026 szeptemberéig.

ÁTTEKINTÉS ÉS SZERVEZÉS

- [ ] Tudjuk, mely termékeink esnek a törvény hatálya alá.
- [ ] Tudjuk, mely régebbi termékeket tartunk még karban (és amelyek ezáltal szintén érintettek).
- [ ] A cégen belül van a CRA témáért felelős személy.

SZOFTVERÖSSZETÉTEL-JEGYZÉK

- [ ] Minden termékhez létezik teljes lista az összes beépített szoftverösszetevőről.
- [ ] Ebben felismerjük az elavult összetevőket is, amelyeket a beszállító már nem tart karban.
- [ ] Ezt a listát folyamatosan naprakészen tartjuk, nem egyszer állítjuk össze.

BEJELENTÉSI FOLYAMAT (KÖTELEZŐ 2026/09-TŐL)

- [ ] Meghatározott, ki veszi észre a kihasznált sebezhetőséget.
- [ ] Meghatározott, ki értékeli és ki jelenti be.
- [ ] A 24 órás határidőt szervezetileg ténylegesen be tudjuk tartani — hétvégén is.

AZ ESZKÖZ MŰSZAKI VÉDELME

- [ ] Az eszközben lévő szoftver titkosítva tárolódik, és nem olvasható ki csak úgy.
- [ ] A frissítések hamisításbiztosak — senki nem juttathat be becsempészett szoftvert.
- [ ] Az eszköz a teljes élettartama alatt kaphat biztonsági frissítéseket.
- [ ] Indításkor az eszköz ellenőrzi, hogy csak valódi, módosítatlan szoftver fut.

BIZONYÍTÉKOK ÉS DOKUMENTÁCIÓ

- [ ] Igazolni tudjuk, hogy a fejlesztés elismert programozási szabványok szerint történt.
- [ ] A megbízhatóság és a támadásbiztonság egy közös koncepcióban van átgondolva, nem külön.
- [ ] A későbbi megfelelőségértékeléshez szükséges dokumentumokat a kezdetektől vezetjük.

4 Hogyan tovább

A következő hónapok döntik el, hogy 2026 szeptemberében rendezett folyamat áll-e majd, vagy sietve kell improvizálni. Aki korán kezd, elosztja a munkát — és elkerüli a határidő előtti drága vészmegoldásokat. A legnagyobb emelő rendszerint nem önmagában a technikában rejlik, hanem a jegyzék, a bejelentési folyamat és az eszközvédelem tiszta összjátékában.

→ Elmélyülés és támogatás

Nemcsak áttekinteni szeretnék a követelményeket, hanem meg is valósítani? Három út:

Szakkönyvek és szoftver

Gyakorlati tudás több mint 35 év beágyazott fejlesztésből — a CRA követelmények mögötti technikai alap. Megtalálható itt: **sc-sarl.com/hu/produkte.html**

Ajándékba: «Képletgyűjtemény informatikusoknak és mérnököknek»

Interaktív HTML képletgyűjtemény, 56 fejezet, kétnyelvű DE/EN, offline használható — ingyen a letöltési részben.

Személyes támogatás

A szoftverösszetétel-jegyzéktől a firmware megerősítéséig. Tanácsadói beszélgetés itt: **sc-sarl.com/hu/kontakt.html**

A termékekhez és letöltésekhez →

Ez az útmutató gyakorlati áttekintést ad, és nem helyettesíti a jogi tanácsadást. Mérvadó az (EU) 2024/2847 rendelet. A határidők állapota: bejelentési kötelezettség 2026.09.11-től, teljes alkalmazhatóság 2027.12.11-től.