EXPERTARTIKEL

CRA, RED OCH CS&R-REGELVERK: Banar väg för en säkrare

Av Francesco Vaiani, Seco

Francesco Vaiani är senior produktmarknadsförare på Seco med fokus på edge AI, inbyggda system och IoT för industrin.

När antalet IoT- och edge-enheter växer ökar också sårbarheterna dramatiskt. Det behövs starka cybersäkerhetsåtgärder som säkerställer oavbruten drift, skyddar data och skyddar användare. Eftersom hotbilden ständigt förändras, utvecklas också de globala regelverken med strängare säkerhetsstandarder.

Europeiska unionen ligger i framkant med **Cyber Resilience Act (CRA)** och **Radiodirektivet (RED)**. Dessa standarder etablerar en omfattande baslinje som formar globala metoder för utveckling av digitala och trådlösa produkter. Många företag står därför inför betydande utmaningar när de anpassar sina affärsstrategier för att uppfylla denna nya uppsättning regler som kommer att krävas för de flesta uppkopplade enheter som säljs inom EU. Liknande regelverk har föreslagits eller redan införts i andra regioner, där Storbritanniens föreslagna **Cyber Security and Resilience (CS&R) Bill** är ett exempel.

Cybersäkerhet omfattar skyddet av enheter, nätverk, firmware och data mot externa hot. Det yttersta målet i IoT-applikationer är att undvika störningar som kan hota drift, säkerhet eller efterlevnad. Samtidigt kan buggar i enheter, föråldrad firmware eller osäkra kommunikationsprotokoll ge angripare en enkel ingångspunkt, vilket gör det möjligt att skapa botnät, stjäla data eller få obehörig kontroll.

Mirai-botnätet kapade till exempel hundratusentals oskyddade IoT-enheter och använde dem för överbelastningsattacker, DDoS. Nyare hot som **Matrix-botnätet** har följt samma mönster och komprometterat allt från hemmaroutrar till telekomutrustning och IP-kameror. Båda fallen visar hur sårbarheter i en enda enhet kan räcka för att kompromettera ett företags globala internetinfrastruktur eller exponera känsliga person- och affärsdata.

Angripare använder allt oftare automatisering för att identifiera och utnyttja sårbarheter i stora nätverk. Framväxten av **AI-drivna cyberattacker** förvärrar problemet genom att skapa mer avancerade hot som också är svårare att upptäcka. För att motverka detta måste företag integrera cybersäkerhet i sina enheter redan från början och göra **security-by-design (SbD)** till en central del av sin strategi.

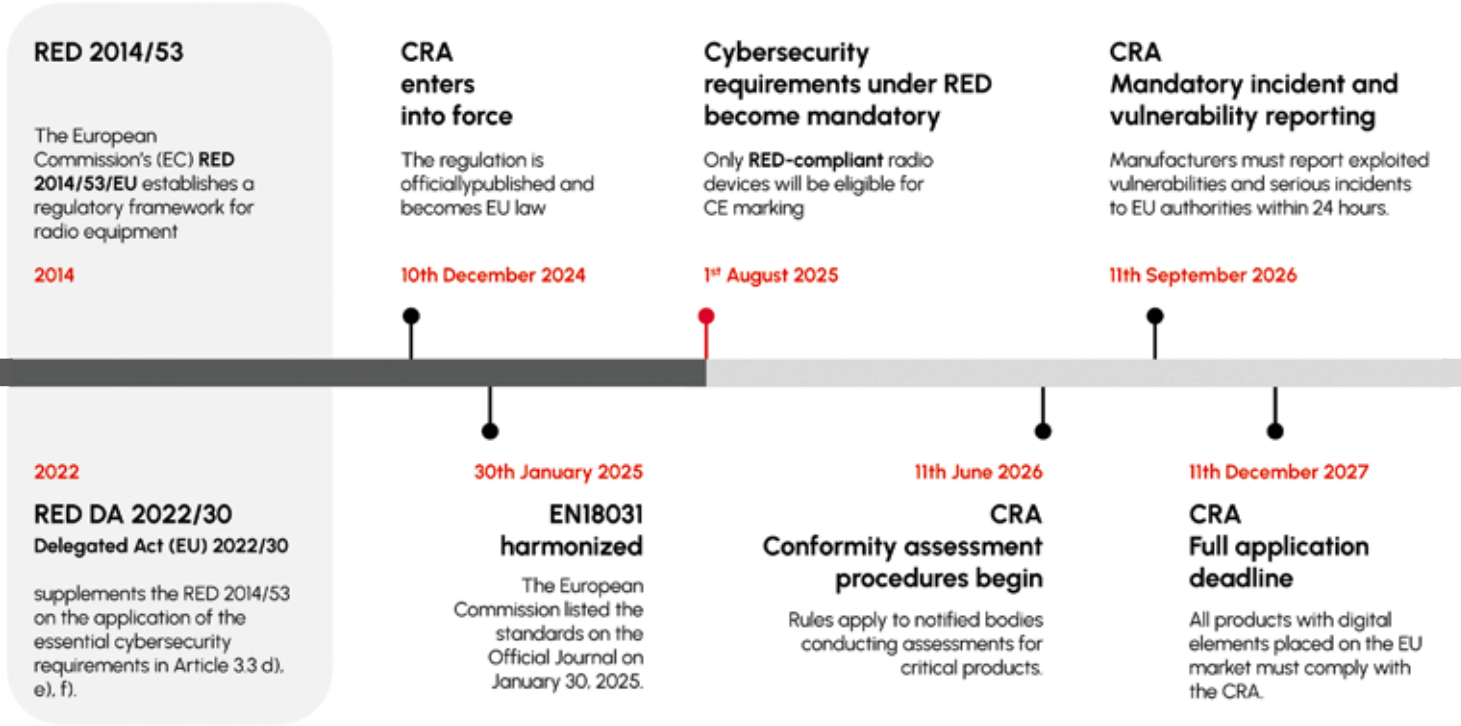
När **Cyber Resilience Act** började gälla den **10 december 2024** markerade den ett viktigt regulatoriskt skifte genom att införa nya cybersäkerhetskrav för nästan alla digitala produkter som säljs inom EU.

Även om de flesta skyldigheter enligt CRA börjar gälla den **11 december 2027**, träder vissa delar i kraft betydligt tidigare. Till exempel måste tillverkare från och med **11 september 2026** rapportera aktivt exploaterade sårbarheter och allvarliga incidenter till EU-myndigheter inom **24 timmar**. Regelverket kräver dessutom att företag utvecklar produkter enligt **SbD-principer**, hanterar sårbarheter under hela produktens livscykel, levererar snabba säkerhetsuppdateringar och upprätthåller omfattande teknisk dokumentation inklusive ingående mjukvarukomponenter, **Software Bill of Materials (SBOM).**

CRA stärker dessutom cybersäkerhetsarbetet genom att rikta sig mot **hela produktens leveranskedja**, från tillverkare till importörer och distributörer. Genom att etablera cybersäkerhet som ett gemensamt regulatoriskt ansvar för dessa aktörer gör åtgärden efterlevnad obligatorisk, vilket i sin tur är en förutsättning för att erhålla **CE-märkning** som krävs för att en produkt lagligt ska få säljas inom EU.

Konsekvenserna av bristande efterlevnad är betydande. Beroende på överträdelsen kan företag drabbas av böter på upp till **15 miljoner euro eller 2,5 procent av den globala årsomsättningen**, beroende på vilket belopp som är högst. Produktförbud och återkallelser är också möjliga. Med tanke på dessa utmaningar innebär en framgångsrik implementering av CRA-principer stärkt kundförtroende samt minskade juridiska och reputationsrelaterade risker.

Figur 1. I princip gäller alla skyldigheter enligt CRA från den 11 december 2027, men vissa bestämmelser börjar gälla redan från 2025 och omfattar både hårdvara och mjukvara ur cybersäkerhetsperspektiv.



uppkopplad värld

I CRA-eran klassificeras produkter som **"default", "important" (Class I och Class II) eller "critical"** vilket kräver omfattande bedömningar av överensstämmelsen.

DESSA KATEGORIER OMFATTAR viktiga enheter och programvara som är avgörande för modern infrastruktur, till exempel:

- Routrar, modem och brandväggar
- Industriella styrsystem och IoT-gateways
- Operativsystem, hypervisorer och container runtime-system
- Identitetshanteringssystem och programvara för privilegierad åtkomst
- Internetanslutna leksaker och bärbara enheter

PARALLELLT MED CRA har EU också skärpt cybersäkerhetsreglerna genom **Radiodirektivet (Directive 2014/53/EU)**. Detta krav gäller alla produkter som säljs inom EU och **avsiktligt sänder eller tar emot radiosignaler**, såsom Wi-Fi, LTE eller Bluetooth.

Från och med **1 augusti 2025** utökade dessutom den delegerade förordningen **2022/30** de obligatoriska cybersäkerhetskraven för tillverkare, vars enheter nu måste:

- Skydda nätverk mot obehörig åtkomst
- Skydda personuppgifter och användarnas integritet
- Förhindra bedrägerier i digital kommunikation

Secos Clea-system har ett brett utbud av verktyg, hårdvara och mjukvara som gör det möjligt för utvecklare att enkelt utrusta sina produkter med de cybersäkerhetsfunktioner som krävs för att uppfylla moderna regelverk.

FÖR ATT FÖRENKLA efterlevnaden utvecklades den harmoniserade standarden **EN 18031**, som ger presumtion om överensstämmelse med RED:s cybersäkerhetsbestämmelser och definierar tekniska krav. Dessa omfattar **secure boot, accesskontroll, krypterad kommunikation och digitalt signerade firmwareuppdateringar**. Det är dock viktigt att notera att denna efterlevnad måste säkerställas **på slutproduktnivå**, inte enbart på modulnivå.

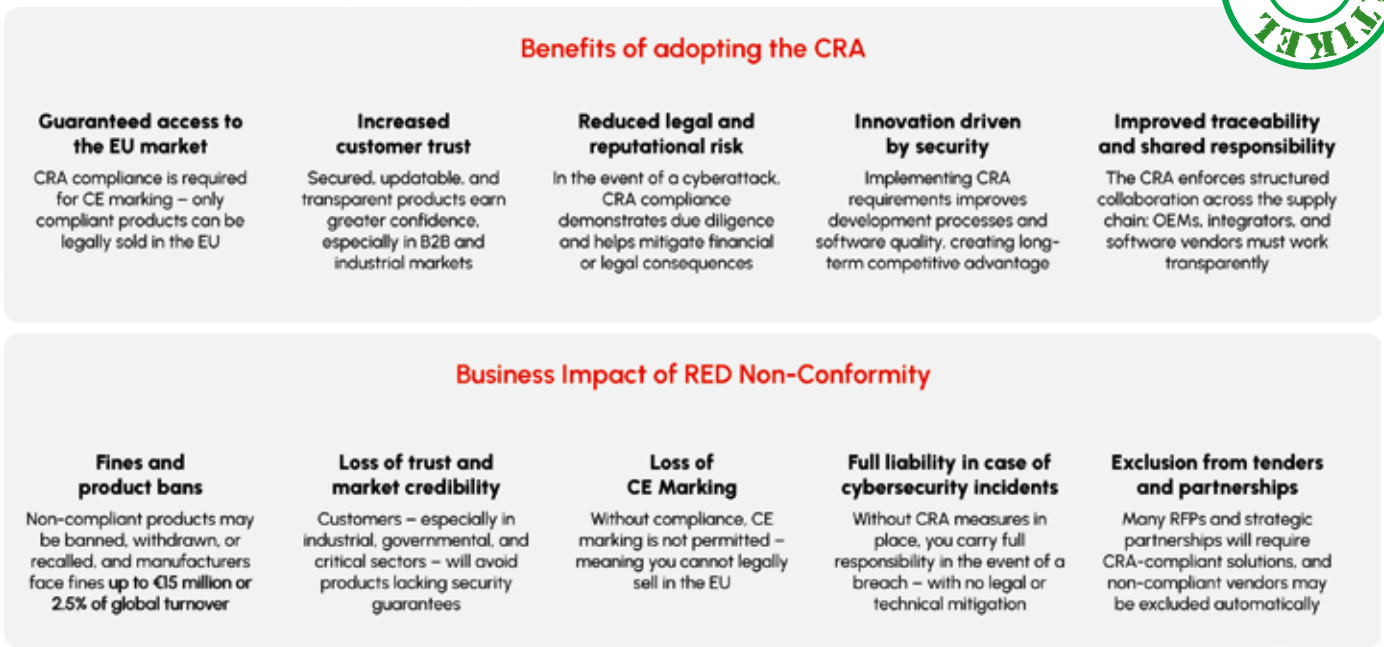
Med ett växande antal CRA- och RED-krav som träder i kraft är cybersäkerhet inte längre valfri utan en förutsättning för inbyggda system och OEM-tillverkare. För ingenjörer innebär detta att säkerhetsdesign och riskanalys måste integreras tidigt i utvecklingsprocessen.

Utöver produktutveckling blir livscykelhantering och operativ efterlevnad avgörande. Tillverkare måste därför kontinuerligt övervaka nya sårbarheter för att snabbt kunna leverera patchar och rapportera allvarliga incidenter inom den föreskrivna tidsramen på 24 timmar.

FÖR ATT MÖJLIGGÖRA detta behöver inbyggda system:

- robusta uppdateringsmekanismer
- krypterad kommunikation
- härdad firmware

EFTERSOM LEVERANSKEDJAN också hålls ansvarig måste varje komponentleverantör kunna bevisa att deras komponenter upp- ▶▶



Figur 2. Jämförelse mellan fördelarna med att följa CRA och riskerna med bristande efterlevnad.

fyller kraven. Annars kan slutprodukten **inte certifieras för laglig försäljning inom EU**, vilket understryker vikten av att integrera cybersäkerhet tidigt i utvecklingsprocessen.

För att effektivt möta dessa växande regulatoriska krav gynnas utvecklare av att använda ett omfattande ekosystem av hårdvara, mjukvara och verktyg designade för inbyggnadstillämpningar. **Secos Clea-plattform** följer exempelvis en **SbD-filosofi** och har grundläggande mekanismer såsom secure boot, krypterad kommunikation och signerad firmware samtidigt som den möjliggör fullständig hantering av produktens livscykel.

EN CENTRAL KOMPONENT för att upprätthålla efterlevnad är **uppdatering över luften**, OTA, vilket ger snabb, tillförlitlig och spårbar distribution av mjukvaru- och firmwareuppdateringar. Genom att leverera regelbundna säkerhetsuppdateringar och snabbt åtgärda exploaterade sårbarheter hjälper Clea tillverkare att uppfylla sina regulatoriska skyldigheter. Det förenklar också skapandet och hanteringen av **SBOM-dokumentation** för CE-efterlevnad och revisioner.

Ekosystemet går ännu längre genom att integrera verktyg för **övervakning, rapportering och efterlevnad**, vilket ger centraliserad kontroll över enhetsflottor, tidig upptäckt av avvikelser samt registrering och rapportering av incidenter. Dessa funktioner effektiviserar arbetsflödet och minskar regulatoriska risker samtidigt som de stärker förtroendet hos kunder och partners som delar ansvaret för efterlevnad.

INTEGRATIONEN av Clea-ekosystemet i ett befintligt embedded-system börjar genom att använda **SDK:er, API:er och agenter** för olika hårdvaru- och mjukvaruplattformar och lägga till dessa i befintliga tekniska stackar. Detta kan göras utan att omdesigna kärnarkitekturen och ger säker kommunikation, enhetsautentisering och livscykelhantering redan i tidiga utvecklingsstadier.

Nästa steg är att ansluta ekosystemet till en molnplattform, till exempel Secos molntjänster, där dashboards och integrationer ger tillgång till funktioner för övervakning, uppdateringar och efterlevnad. Dessa plattformar stöder standardiserade protokoll och integreras i befintliga utvecklings- och driftsprocesser för att säkerställa skalbarhet över stora och heterogena enhetsflottor.

FÖR ATT FÖRENKLA DRIFT erbjuder Clea även **DevOps- och säkerhetsverktyg** för automatisk SBOM-generering, sårbarhetsskanning, loggning och rapportering. Detta gör det möjligt för team att uppfylla dokumentations- och revisionskrav direkt i sina verktygskedjor, vilket minskar manuellt arbete och förkortar **time-to-market för kompatibla produkter**.

Med införandet av **CRA och RED** blir cybersäkerhet ett grundläggande krav för embedded-system och OEM-företag som vill sälja i EU-länder. **Security by design, kontinuerlig livscykelhantering, SBOM-dokumentation och snabb incidentrespons** är nu obligatoriska, vilket innebär att utvecklare måste integrera säkerhet på arkitekturnivå samtidigt som OEM-företag säkerställer efterlevnad i hela leveranskedjan. ■