Ridå upp för första akten i CRA

EXPERTARTIKEL

Av Cedric Vincent, Tria Technologies

Cedric Vincent chefar över Software Technology Lab på Tria Technologies. I två decennier har han kodat inbyggda system på Linux, vilket för närvarande handlar mycket om AI-skiftet från moln till edge. På Linkedin kan du se honom utforska LLM-baserade utvecklingsverktyg.

Cyberattacker blir allt vanligare – och allt allvarligare – i en allt mer digital värld. De är en fara för både tillverkare och leverantörer. Och för samhället som helhet.

År 2022 hamnade hotet från hackarna i strålkastarljuset på den digitala scenen i Storbritannien när ett säkerhetshål avslöjades i Kinatillverkade övervakningskameror. De var installerade på kontor, i offentliga miljöer och till och med på myndigheter.

År 2026 är frågan ännu viktigare. Uppkopplade produkter får allt större spridning i takt med att städerna blir smarta. Cyberattacker med allvarliga konsekvenser kan ske i allt större skala. Behovet av lösningar är akut.

Ett färskt exempel är globala klädes- och matvarukedja Marks & Spencer. Påskhelgen förra året drabbades den av en cyberattack mot sin handel, sina kontaktlösa betalningar och sin logistik.

Näthandeln var nedstängd i 46 dagar. Hackarna kom åt kunddata i form av namn, e-postadresser och bostadsadresser (bankuppgifter ska inte ha läckt). Kostnaden för intrånget beräknas i efterskott till nära fyra miljarder kronor (300 miljoner pund). Utredningen pekade på att intrånget troligen skedde via företagets IT-leverantör.

En akut kris

Dessa attacker är bara några exempel på vad som möter företag och privatpersoner varje dag jorden runt. För att ta itu med en allvarlig kris sjösatte EU i slutet av förra året CRA (Cyber Resilience Act).

Den kompletterar befintlig EU-lagstiftning inom cybersäkerhet. Där finns sedan januari 2023 NIS 2-direktivet med krav på riskhantering, incidentrapportering och ansvarsutkrävande. EU-kommissionen driver även EUVD, en sårbarhetsdatabasen som hålls uppdaterad med rapporter från betrodda källor.

Notera den viktiga distinktionen att ett ”direktiv” anger ett mål som EU-medlemsstaterna ska uppnå. De får själva välja hur. En akt däremot (en ”förordning”) – som CRA – är däremot en bindande lag med specifika regler som skall följas. I den meningen går CRA betydligt längre. Kommissionen säger att akten ska ”höja nivån på cybersäkerhet för produkter med digitala komponenter” och kräver att tillverkare och återförsäljare säkerställer cybersäkerhet ”under hela produkternas livscykel”.

Ansvaret för säkerhet hamnar på tillverkaren, som måste se till att hårdvara och mjukvara uppfyller gällande krav innan produkten släpps in på EU-marknaden. Därefter är fortgående säkerhetsuppdateringar obligatoriskt, liksom incidentrapportering och tredjepartsgranskning. En CE-märkning dokumenterar att CRA efterlevs.

Innan vi går vidare till vad akten konkret kräver är det värt att notera att den inte enbart välkomnats med öppna armar. Kritiken handlar bland annat om att perspektivet varit för generellt – att CRA har ett one-size-fits-all-perspektiv med samma krav för vitt skilda produkter – från smarta klockor till babymonitorer. En vanlig synpunkt som Tria hör från sina kunder är att full CRA-regelefterlevnad skulle driva dem till konkurs.

För egen del är den största oron att akten, om den skulle tillämpas fullt ut, skulle kunna bromsa innovationstakten i Europa avsevärt.

Akten kräver att företag redovisar alla utnyttjade sårbarheter till myndigheter inom 24 timmar.

Kritiker menar att detta krav faktiskt kan öka risken för cyberattacker, eftersom det skapar en databas i realtid över säkerhetshål. De uttrycker farhågor för att stater kan utnyttja redovisade sårbarheter för underrättelse- eller övervakningssyften.

Syftet med CRA

Oavsett vad man tycker om CRA så är den här nu. Utvecklare och OEM-tillverkare behöver ha en klar bild av vad lagstiftningen täcker och vad den kräver. Datromodulexperten Tria Technologies anser att det är avgörande att branschens nyckelspelare känner till sitt ansvar under CRA. Målet för oss är att tillverkare som arbetar proaktivt med CRA ska kunna navigera cybersäkerhetslandskapet effektivt, skydda sin verksamhet och bidra till ett robust ekosystem för tillverkare.

Enligt EU-kommissionen:

- CRA tar itu med ”den otillräckliga cybersäkerhetsnivån i många produkter och bristen på säkerhetsuppdateringar i rätt tid”.
- Den tar också itu med ”de utmaningar som konsumenter och företag för närvarande står inför när de försöker avgöra vilka produkter som är cybersäkra”.
- Förordningen ställer tvingande cybersäkerhetskrav på tillverkare och återförsäljare i varje led av leveranskedjan av en produkt, specifikt planering, design, utveckling och underhåll. Huvudmålet är ”Secure by Design”, det vill säga att system, programvara och tjänster ska byggas med säkerhet inbyggd från början – inte tillagd i efterhand.
- Vissa produkter ”av särskild relevans för cybersäkerhet” måste genomgå en tredjepartsbedömning av ett auktoriserat organ innan de får säljas på EU-marknaden.

Reglerna gäller produkter som är uppkopplade eller anslutna till andra produkter, direkt eller indirekt. Undantag görs för viss öppen källkod och vissa tjänster som redan omfattas av befintliga regelverk, som medicintekniska produkter, luftfart och bilar.

Fördelar med CRA

CRA ska ge ökad säkerhet och väsentligt lägre risk för cyberattacker. CRA skyddar företag och konsumenter mot dataintrång och dåligt PR. Det finns ett rent ekonomiskt perspektiv: CRA förebygger de kostnader som dataintrång skulle medföra – vi har redan sett kända företag drabbas.

Tria har under en längre tid samarbetat nära med kunder för att säkerställa efterlevnad av den nya förordningn. Målet är att kundernas produkter ska uppfylla CRA-kraven i hela leveranskedjan från komponent till färdig produkt. En av de viktigaste fördelarna Tria kan erbjuda är förtroende. Genom att arbeta med ett enda bolag — som hämtar expertis från partners som Qualcomm, NXP, Intel och Renesas — kan konstruktörer och OEM-tillverkare vara trygga med att de har tillgång till skräddarsydda inbyggnadslösningar i varje steg.

EU:s cybersäkerhetsakt ställer tuffa krav på de som är involverade i konstruktion, tillverkning och leverans av digitalt baserade produkter.

Deadline 2027 närmar sig. Bristande efterlevnad kan ge kännbara böter – för närvarande 15 miljoner euro eller 2,5 procent av global omsättning.

Vad gäller tidsschemat träder CRA:s huvudsakliga skyldigheter i full kraft den 11 december 2027. Men nedräkningen började redan den 10 december 2024 när akten officiellt började gälla. Från och med i höst, den 11 september, gäller rapportskyldighet: inom 24 timmar måste du informera myndigheter om aktivt utnyttjade sårbarheter. Incidenter måste rapporteras inom 72 timmar.

Det är alltså hög tid att agera – inte bara för att vara helt redo när datumen infaller, utan framför allt för att minska framtida risk för allvarliga cyberattacker och slippa de astronomiska kostnader som efterspelet innebär. ■

För mer information: