CRA-säkrad inbyggnadsarkitektur

EXPERTARTIKEL

Författare: Sysgo

EU:s Cyber Resilience Act (CRA) håller i grunden på att förändra cybersäkerheten för digitala produkter i och med att säkerhet går från att vara en ”funktion” till att bli ett kärnkrav. Förordningen kräver säkerhet i hela kedjan, från design, proaktiv hantering av sårbarheter och transparens i leverantörskedjan till ett tillförlitligt, långsiktigt uppdateringsstöd under hela produktens livscykel.

För utvecklare och systemintegratörer i säkerhetskritiska sektorer som järnväg, flyg, försvar och industriell automation kan dessa krav vara överväldigande. Tyska Sysgo, som utvecklar säkerhetskritiska realtidsoperativsystem, vill gärna vara en strategisk partner i denna omställning.

FÖRETAGETS ARKITEKTUR bygger på att operativsystemet är så kallad Root of Trust. För att säkerställa det används två komponenter:

- **PikeOS (Realtidsoperativsystem och hypervisor):** Utvecklat med en separationskärna som säkerställer strikt rumslig och tidsmässig isolering mellan kritiska och icke-kritiska funktioner. Detta förhindrar felpropagering, minimerar attackytan och möjliggör oberoende verifiering av komponenter. PikeOS är dessutom certifierat enligt Common Criteria EAL5+, vilket ger en hög tillitsnivå och förenklar dokumentations- och granskningsprocesser enligt CRA.
- **ELinOS (Embedded Linux):** Linux är avgörande för modern uppkoppling så ELinOS är utformat för att göra det möjligt att ta bort onödiga tjänster och lämna endast den nödvändiga koden, vilket kraftigt minskar attackytan. Funktioner som en immutabel OS-arkitektur och stöd för containrar skyddar mot manipulation under drift och säkerställer att kärnsystemet förblir säkert även när applikationer uppdateras.

EN BETYDANDE UTMANING med CRA är kravet på att underhålla produkter under hela deras livscykel. Sysgo hanterar detta genom:

- **CVE-hantering (Common Vulnerabilities and Exposures):** Det finns långsiktiga underhållsgrenar med bakporterade säkerhetsuppdateringar – ofta över 15 år – vilket sträcker sig långt bortom normala supportcykler i open source-communityn.
- **Strukturerad incidenthantering:** Det finns ett informationssäkerhetsledningssystem (ISMS) certifierat enligt ISO 27001 samt ett dedikerat PSIRT-ramverk. Detta säkerställer att mottagning av sårbarheter, prioritering och samordnad åtgärdshantering sker transparent och professionellt.
- **Proaktiv rapportering:** Kunder får regelbundna säkerhetsbulletiner, detaljerade ändringsloggar och patchdokumentation, vilket gör det möjligt för tillverkare att visa på aktivt säkerhetsunderhåll gentemot tillsynsmyndigheter och slutanvändare.

CRA KRÄVER ATT TILLVERKARE förstår och har kontroll över sina programvarukomponenter från tredjepartsleverantörer. Arbetet förenklas genom att automatisera skapandet av högkvalitativa artefakter:

- **Automatiserad SBOM-generering:** Både PikeOS och ELinOS kan generera en Software Bill of Materials i standardformat som SPDX. Detta gör att utvecklingsgruppen kan spåra beroenden, hantera open source-licenser och identifiera sårbarheter på komponentnivå.
- **Kontrollerad integration:** Genom att utnyttja en modulär arkitektur blir resultatet en säker konsolidering av arbetslasterna. Utvecklarna kan köra säkerhetskritiska styrloopar på PikeOS samtidigt som moderna, containeriserade applikationer körs på ELinOS – allt på en och samma systemkrets. Detta minskar hårdvarubehovet och förenklar den säkerhetsargumentation som krävs för efterlevnad.

DET FINNS OCKSÅ ITAR-fri programvara som är 100 procent europeisk. I ett geopolitiskt klimat där suveränitet i leveranskedjan blir allt viktigare innebär detta att högsäkerhetsprojekt inom försvar och kritisk infrastruktur förblir oberoende av utländsk jurisdiktion, vilket förenklar både internationell efterlevnad och driftsättning. ■