Cybersikkerhed med omtanke

Prevas tilbyder en lang række services relateret til integration af cybersikkerhed i produkter, applikationer og processer, og ifølge udviklingshuset gælder det om at følge de standarder, der findes på området, så langt det overhovedet er muligt.

Af Lars Kristiansen

Cybersikkerhed er en problemstilling, der for længst er blevet et særdeles vigtigt tema for alle, der er involveret i udvikling, test og produktion af elektronikprodukter, som på den ene eller anden måde er opkoblet til internettet og dermed potentielt er sårbare over for cyberangreb.

Den mindste 'sprække' i selv det mest simple produkt, der f.eks. er opkoblet til et større netværk, kan repræsentere et kæmpemæssigt sikkerhedsproblem, der i tilfælde af et cyberangreb kan give tilgang til en virksomheds datanetværk og dermed videre til alle opkoblede enheder og i værste fald blotte vitale data eller helt lamme virksomhedens drift.

Cybersikkerhed repræsenterer et bredt område og er grundlæggende en særdeles tværfaglig problemstilling, som samtidig er ekstrem dynamisk. Der introduceres nærmest dagligt nye cybersikkerheds-risici, der (måske) skal tages højde for i produkter og services.

- Man kan sige, at integration af datasikkerhed i produkter og systemer på mange måder minder om EMC-problematikken for mange år tilbage. Ligesom EMC berører datasikkerhed på et eller andet niveau stort set alle produkter. Men det er et område – som EMC i sin tid – der ofte ligger uden for

- I forbindelse med vores apparat patching services udfører vi automatiserede regressionstest for stadig flere kunder og deres produkter, og der er tale om mange forskellige produkter, der rækker lige fra de mest simple til mere komplekse, forklarer Rune Hillebo Wiinberg, der er 'Head of Cybersecurity' i udviklingshuset Prevas.

de enkle firmaers kernekompetencer, og derfor søger mange virksomheder – både store og små – ekstern support i forbindelse med sikring af apparater, systemer, data og services, forklarer Rune Hillebo Wiinberg, der er 'Head of Cybersecurity' i udviklingshuset Prevas.

Som elektronik- og apparatudviklingshus med en bred vifte af kunder i mange forskellige segmenter har Prevas i en årrække haft fokus på cybersikkerhed – specielt med fokus på de internationale standarder, der allerede findes og de krav og standardiseringer, der er på vej.

- Vi oplever en øget efterspørgsel hos kunder, der i stigende grad ser cybersikkerhed som en vigtig parameter i forbindelse med udvikling og salg af nye enheder, og vi har opbygget stor erfaring i integration af cybersikkerhed i produkter, systemer og processer inden for forsvar, medicinsk udstyr og energi. Den erfaring, vi har opbygget her, kan vi også bruge til at adressere den stigende interesse inden for sektorer som forbrugerelektronik og hele det vidtrækkende IoT-område, som vi oplever i øjeblikket, fremhæver Rune Hillebo Wiinberg.

Tværfaglig proces

At bygge sikkerhed ind i produkter er i høj grad en tværfaglig proces, som ikke alene handler om at engagere software og hardwarefolk, men i ligeså høj grad QA-folk og produktionsmedarbejdere. Man kan betegne det som en slags procesøvelse, der kræver viden og input og handling fra alle dem, der på den ene eller anden måde er beskæftiget med udvikling, test og certificering samt produktion af elektronik.

Grundlæggende kan man sige, at der i forbindelse med indbygning af cybersikkerhed i apparater og enheder er tre grundlæggende 'risiko-elementer', som der helt fra starten skal fokuseres på, påpeger Rune Hillebo Wiinberg:

1. Kravene til sikkerheden på apparatniveau skal analyseres og fastlægges. Der kan om nødvendig vælges implementeringer med secure-boot, krypteret RAM eller secure microcontrollere eller andre hardware/firmware-orienterede sikkerhedstilgange.
2. Der skal også laves en vurdering af de anvendelsesmiljøer, som apparatet kommer til at indgå i og dermed afdække de potentielle sikkerhedsrisici, der skal tages højde for i forbindelse med cybersikkerheds-implementeringen. Dette punkt kan være vanskeligt, fordi mange produkter typisk kan anvendes i mange sammenhænge, der på forhånd kan være svære at afdække fuldstændig.
3. Endelig skal der med kritiske øjne ses på de potentielle datarisici i forbindelse med udviklingsprocessen og ikke mindst produktionsprocessen, som i mange virksomheders tilfælde foregår hos eksterne samarbejdspartnere, hvilket gør det ekstra vigtigt, at der er 100 procent styr på alle de sikkerhedsmæssige aspekter i forbindelse med f.eks. programmering.

- Prevas ser cybersikkerhed som en samlet pakke, hvor der er fokus på både apparat-

...FORTSÆTTES NÆSTE SIDE

FORTSAT FRA SIDE 11:

sikkerhed, apparatets miljø samt de udviklings- og produktionsmiljøer, hvor apparatet skal fremstilles og opdateres. Vi sælger cybersikkerhed som en ydelse, hvor vi både kan gå ind i hele processen og i enkelte dele af arbejdet. En af de store fordele er, at vi gennem vores involvering i mange forskellige projekter og faser af cybersikkerheds-processen har opbygget en bred vifte af kompetencer, som det vil være svært for mange virksomheder – i hvert fald de lidt mindre – at opbygge og løbende vedligeholde, siger Rune Hillebo Wiinberg.

Stigende lovkrav til cybersikkerheden i organisation og apparater

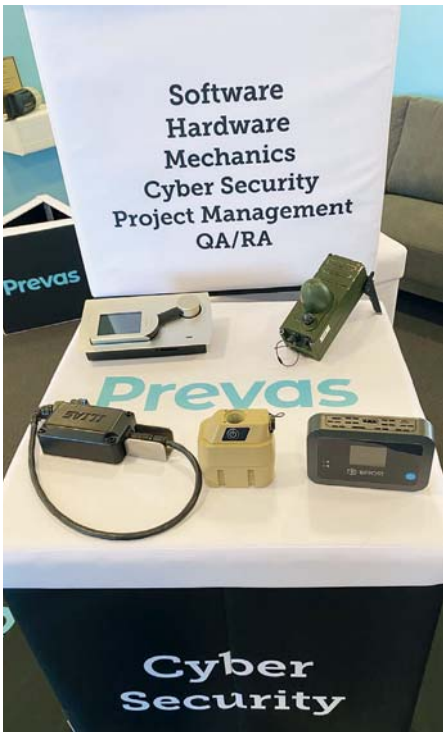
Der er i øjeblikket fokus på bl.a. EU's NIS2 forordning, hvis formål er at styrke og ensarte cybersikkerheden og modstandsdygtigheden over for cybertrusler i virksomheder og offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet.

Et andet særdeles vigtigt nyt EU-initiativ er den såkaldte Cyber Resilience Act (CRA), der i EU-regi blev officielt vedtaget i december 2023. CRA dækker over et juridisk framework, der beskriver cybersikkerhedskrav til hardware og software med digitale elementer (det vil sige stort set alle typer elektronikprodukter), som markedsføres inden for EU.

Der er også introduceret en markant tilføjelse til radio-direktivet, RED, i form af RED DA, hvor der bl.a. er fokus på udbygget cybersikkerhed i forbindelse med radiokommunikation. RED DA blev vedtaget i 2022 og træder endelig i kraft 1. august 2025.

Der bliver her bl.a. stillet krav om, at produkter med indbyggede kommunikationsfaciliteter skal inkludere sikkerhedsfeatures, der sikrer, at de ikke kan skade andre opkoblede enheder og applikationer og samtidig fuldt ud kan garantere personlig data-privacy i forbindelse med kommunikationen.

- CRA, NIS2 og ændringerne i RED har alle til formål at øge cybersikkerheden i organisationer, apparater og OT (Operationel Technology) systemer på europæisk plan. Selv om de præcise krav endnu ikke er på plads, så forventer vi på apparatniveau bl.a. krav til patch management, hvor virksomheder i fremtiden proaktivt skal kunne levere softwareopdateringer for at lappe huller i sikkerheden i takt med, at de bliver offentliggjort, hvilket er en stor ændring, som alle virksomheder allerede nu bør begynde at forberede sig på, understreger Rune Hillebo Wiinberg.



Standarder er rygraden i de fleste projekter

Der er søsat mange standardiserings-aktiviteter inden for cybersikkerhedsområdet, der fokuserer på forskellige aspekter i forbindelse med apparatopbygning og processer. Nogle færdige – eller er på vej til at være det – mens andre endnu er under opbygning. Nogle er mere generiske, mens andre (i nogle tilfælde undergrupper af de mere generiske) sigter mod mere specifikke produktsegmenter og anvendelser.

- Cypersikkerhed kan være svært at forstå og implementere i praksis, men der findes efterhånden mange standarder, der kan gøre det hele lettere og mere strømlinet. Vi anbefaler helt klart, at man i forbindelse med et cybersikkerhedsprojekt i så høj grad, som det er muligt, tager udgangspunkt i de standarder og de generelle anbefalinger, som allerede er tilgængelige, understreger Rune Hillebo Wiinberg.

En af de eksisterende cybersikkerhedstandarder, der ifølge Rune Hillebo Wiinberg bruges i mange sammenhænge, er IEC 62443, der som udgangspunkt fokuserer på sikkerheden inden for industrielle netværk. Under IEC 62443 er der på nuværende tidspunkt defineret ni understandarder, tekniske rapporter og tekniske specifikationer.

IEC 62443 standardserien er udviklet til at sikre industriel automation og tilhørende kontrolsystemer, men standarderne bliver også brugt i en stadig bredere vifte af anvendelsesdomæner som energiforsyning, distribution og i skibe med mere. Implementering af IEC 62443 kan forhindre eller afbøde konsekvenserne af et cyberangreb og forøger sikkerheden gennem hele produktet/systemets livscyklus.

- Selvom IEC 62443 har sine rødder i den 'tunge' industri, ser vi også, at den desuden finder anvendelse i andre sammenhænge – den giver f.eks. afsæt til IEC 81001-5-1 standarden til medicoprodukter og anvendes også flittigt til andre forbundne konsumerprodukter. Grundlæggende er det vores budskab, at det gælder om at tage afsæt i den standardisering, der findes og er relevant i den aktuelle applikation – uanset om standarden oprindelig er tænkt til andre typer af anvendelser, påpeger Rune Hillebo Wiinberg.

IEC 62443 adresserer også arbejdsprocesser og medarbejderuddannelse og ansvar. Der arbejdes med andre ord med en mere holistisk tankegang ud fra den kendsgerning, at alle sikkerhedsmæssige risici ikke nødvendigvis er teknologi-baserede – men i høj grad også relaterer til den uddannelse og træning, som medarbejderne har fået i forbindelse med de sikkerhedsmæssige processer og rutiner.

Håndtering gennem hele livscyklussen

Integration af cybersikkerhed i et produkt eller en applikation er i høj grad en dynamisk proces, der i langt de fleste tilfælde strækker sig over hele produktets levetid. Der kræves således som nævnt konstant overvågning af nye sikkerhedsmæssige sårbarheder, og software og operativsystem skal løbende opdateres i de tilfælde, hvor det skønnes nødvendigt.

- Når man betragter cybersikkerhed over hele produktets livscyklus, så er der naturligvis en række vedligeholdsomkostninger, som man allerede fra starten skal tage

højde for. Forskellige firmaer har naturligvis forskellige modenhedsniveauer, når det gælder implementering af cybersikkerhed i produkter og processer. Men det er vores erfaring, at specielt mindre firmaer ofte ikke er fuldt beviste om, hvad det indebærer at holde produkter konstant opdaterede, siger Rune Hilleborg Wiinberg, der fortsætter:

- Det er også derfor, at vi tilbyder alle firmaer – uanset deres kompetencer og størrelser – at holde øje med nye sikkerheds 'patches', der gennem vores kendskab til kundens produkter eller systemer på den ene eller anden måde muligvis kan påvirke deres produkter. På den måde kan vi løbende udrulle velafprøvede og patchede firmware-opdateringer direkte til kundernes apparater. Ved at overlade en stor del af cybersikkerheden til Prevas kan kunderne koncentrere sig om at udvikle apparaternes grundlæggende kvaliteter. Prevas' service er et tilvalg til Prevas Industrielle Linux (PIL), men den kan også tilbydes til andre systemer – uanset om de er udviklet af Prevas eller ej, forklarer Rune Hillebo Wiinberg.

Han understreger, at selv om der offentliggøres en ny sikkerhedspatch i f.eks. en NIST database, der har relation til software, som en kunde bruger, så er det ikke altid, er der er behov for ændringer eller modifikationer, fordi sårbarheden ikke nødvendigvis har betydning for produktet og dens funktionalitet i det aktuelle produkt.

- Men det vigtige i den forbindelse er, at der løbende laves vurderinger af produktsikkerheden, når der identificeres nye sårbarheder, og det er denne proces, vi er med til at understøtte gennem vores service, siger Rune Hillebo Wiinberg.

Hvis og når det er nødvendigt at lave sikkerhedsmæssige eller andre opdateringer, så er det typisk nødvendigt at gennemføre funktionelle tests – de såkaldte regressionstest – der skal sikre, at softwareændringerne ikke på den ene eller anden måde samtidig ændrer funktionaliteten eller introducerer fejl, hvilket selvfølgelig ikke er acceptabelt.

- Vi udfører automatiske regressionstest for stadig flere kunder og deres produkter, og der er tale om mange forskellige produkter, der rækker lige fra de mest simple til mere komplekse. Hele livscyklus-aspektet er vigtigt og bliver endnu vigtigere, når kravene skærpes yderligere, og derfor er det også afgørende, at virksomhederne helt fra starten tager omkostningerne gennem hele produktets levetid med ind i den samlede omkostningsstruktur for det pågældende produkt, forklarer Rune Hillebo Wiinberg.

Sikker – men ikke 'oversikker'

Det er åbenlyst, at cybersikkerhed på hver sin måde påvirker alle produkter, applikationer og processer. Men når det er sagt, så er det også vigtigt, at man ikke introducerer 'unødvendig' sikkerhed.

- Sikkerheden er afgørende, men den må ikke være en hæmmende faktor i forbindelse med udviklingsprocessen, som kan føre til unødvendige 'trade-of' mellem 'usability' og sikkerhed og også højere udviklingspriser og i yderste konsekvens også mindre attraktive produkter set fra kundens side, siger Rune Hillebo Wiinberg.