Udvælgelsesguide til cybersikkerhedsstandarder

Sådan udvælger du den rette cybersikkerhedsstand, når du udvikler IoT-produkter.

Når man udvikler produkter, der kan kobles på internettet, er det vigtigt at vurdere IoT-produktets cybersikkerhed. Der findes flere forskellige standarder, man kan tage udgangspunkt i, når man skal håndtere cybersikkerhed. Her er en guide til udvælgelsen.

Tag udgangspunkt i markedskravene

Det første man skal være opmærksom på, når man udvælger, hvilke cybersikkerhedsstandarder man skal anvende, er, om der er nogle markedskrav, der er gældende. Det kan være regulatoriske krav eller de-facto branchekrav, som kunder, brancheorganisationer eller forsikringsselskaber forventer, man lever op til.

Samtidig er det vigtigt at huske, at mange af de eksisterende standarder indeholder mange af de samme funktionelle krav. Altså de krav, der stilles til implementeringen af produktet, fx håndtering af kodeord, kryptering og software-opdatering.

ETSI EN 303 645 – primært for konsumer IoT-produkter

Standarden ETSI EN 303 645 har sit primære fokus på *konsumer IoT*-produkter, fx vaskemaskiner, smarthome-produkter og legetøj. Standarden er simpel i sit udtryk og har stort fokus på at være nem at anvende.

Der stilles en række simple, funktionelle krav til produktet, for hvad der skal være implementeret. Disse funktionelle krav er angivet i denne tabel:

Funktionelle krav:	
• Ingen universelle standardkodeord • Hold software opdateret • Gem følsomme data sikkert • Kommunikér sikkert • Minimér eksponerede grænseflader • Sikre integritet af software	• Sikre persondata • Håndtering af udfald • Undersøg telemetridata • Gør det let for brugere at fjerne deres data • Gør installation og vedligehold nemt • Validér input data

Der er desuden krav om, at man har implementeret en metode for, hvordan brugere og andre kan indrapportere fundne sårbarheder i produktet.

Til denne standard er ETSI ved at udvikle et rammeværk for, hvordan man kan validere, at kravene er overholdt i form af ETSI TS 103 701. Dette rammeværk beskriver, hvordan man opbygger sin dokumentation i et struktureret format, så der kan udarbejdes en standardiseret testplan for, hvordan de underliggende krav kan valideres af enten interne eller eksterne parter.

UL2900-1 – en generisk standard for cybersikkerhed

UL2900-1 er en mere generisk standard i forhold til ETSI EN 303 645. Med fokus på netværks-konnekterbare produkter kan denne standard dække nærmest alle typer af produkter, der har en form for datakommunikation. Den store forskel er, at UL2900-1 tager direkte udgangspunkt i en risikoanalyse af produktet og dens tilsigtede brug. Det bevirker, at processen kan være tungere at komme i gang med, hvis man ikke har lavet risikoanalyser tidligere. Man

skal nemlig både havde styr på potentielle trusler overfor produktet, og man skal kunne dokumentere sin analyse-proces overfor en assessor, der skal validere produktets overholdelse af standarden.

Dette skal dog ikke være en afskrækkelse, da det bevirker, at man opnår en mere dybdegående indsigt i, hvad det er, der skal beskyttes i produktet, hvilke trusler der er overfor produktet samt muligheden for kun at bruge udviklingsressourcerne der, hvor det er nødvendigt.

Til grundstandarden findes der desuden et par andre standarder med krav til specifikke produkttyper: UL2900-2-1 til sundhedsprodukter, UL2900-2-2 til industrielle systemer (stadig et udkast) og UL2900-2-3 til alarm og sikringssystemer.

IEC 62443 – specifikt for industri og søfart

Hvis man udvikler produkter, der skal benyttes i et industri- eller søfartsmiljø, kan det være relevant at kigge på IEC 62443-serien. Denne serie er specifikt udviklet til industrielle automationssystemer og dækker flere områder inden for cybersikkerhed. Serien tager tre tilgangsvinkler: produktudvikler, integrator og ejer. Med disse tre opbygges et økosystem for, hvordan cybersikkerhed håndteres i hele kæden.

For **produktudvikleren** findes IEC 62443-4-1 og IEC 62443-4-2. Standarden IEC 62443-4-1 omhandler udviklingsprocesserne, omkring hvordan man håndterer implementeringen af de funktionelle sikkerhedskrav, der ligger i IEC 62443-4-2. Der er altså en række proceskrav, man skal være klar over, inden man kaster sig ud i at implementere funktioner fra IEC 62443-4-2. Dette gøres blandt andet ved 62443's egen implementering af et CMMI-lignende system (Capability Maturity Model Integration system).

I standarden er der dog taget højde for, at det kan tage lang tid at opnå et proces-teknisk niveau, hvor der er styr på alle de krav, der stilles i IEC 62443-4-1 Det er ikke et krav, at man har opnået et bestemt niveau for at kunne udvikle produkter, der overholder IEC 62443-4-1 og 4-2, men det kan give en indikation af, hvor stort et arbejde, det vil være at komme i gang med og gennemføre udviklingsarbejdet.

For **integrator** og **ejer af systemer** findes flere standarder i serien til håndtering af kravspecifikation til et specifikt anlæg, samt krav til drift og vedligehold. Dette ligger uden for scope af denne vejledning.

Serien opstiller fire sikkerhedsniveauer, som - i en simpel form - benyttes til at beskrive, hvilke sikkerhedsforanstaltninger, der er lavet i et specifikt produkt. Det gør det let at kommunikere, hvad der sikkerhedsmæssigt er muligt med produktet, så en integrator nemt kan se, om et produkt kan benyttes i en bestemt opsætning, eller om der eventuelt skal lave yderligere tiltag omkring produktet for at opnå den ønskede sikkerhed.

Andre cybersikkerhedsstandarder og guidelines

Når man udvælger standarder til håndtering af sit produkts cybersikkerhed, kan det være relevant at se på, hvilke nye standarder indenfor produktsikkerhed, der er under udvikling, fx ISO 27400 og ISO 27402, som begge har fokus på sikkerhed og privacy i IoT-systemer. Hvis man allerede benytter ISO 27001 i sin organisation, kan det være relevant at følge udviklingen af disse nye standarder.

Ligeledes findes der et stort udvalg af 'guidelines of frameworks' til at hjælpe med sikkerheden i IoT-produkter, blandt andet fra IoT Security Foundation og OWASP, som kan være gode at se nærmere på.

Hvilken cybersikkerhedsstandard skal man vælge?

Indledningsvist er det vigtigt at gøre sig klart, hvor mange ressourcer man kan bruge på cybersikkerhed, inden man vælger en retning. Som med alt andet opnår man sjældent en fornuftig løsning, hvis ikke ressourcer, ambition og behov er afstemt. Man skal altså havde en plan for, hvordan man skal udvikle sine processer omkring cybersikkerhed.

Her er det vigtigt at huske, at cybersikkerhed ikke er et mål, der kan nås, men en kontinuerlig proces, der skal holdes opdateret, ved at man regelmæssigt ser på, hvordan verden har ændret sig i forhold til det billede, man lavede den oprindelige proces ud fra. Det kan være fornuftigt ikke at gabe for stort, men at forsøge at finde et passende niveau, som matcher de kompetencer man har med de behov, der er for cybersikkerheden.

Basal håndtering af cybersikkerhed

Har man ikke arbejdet med cybersikkerhed før, kan et godt udgangspunkt være at tage fat i ETSI EN 303 645 og se på de krav, der er stillet. Det kan give et indblik i, hvad der som minimum bør være på plads. Det kan med fordel kombineres med underbyggende kodeanalyse og sårbarhedstest for at give en højere tiltro til, at man har implementeret løsninger fornuftigt, og at produktet ikke har medfødte sårbarheder, man ikke kan acceptere.

Man kan udbygge denne løsning med ETSI TS 103 701 om er et rammeværk for opbygning af dokumentationen til at sikre, at man er kommet ordentligt omkring de funktionelle krav i ETSI EN 303 645.

Dybere analyse af cybersikkerhed

Hvis der er behov for en dybere analyse af sikkerhedsbehov samt underbyggende test og dokumentation, kan der være mere relevant at se på UL2900-1. Implementeringen af sikkerhedsfunktioner er baseret på den underliggende risikoanalyse, og det er krævet, at der udføres kodeanalyse samt penetrationstest for at sikre, at de ting, som kan være accepteret i risikoanalysen, stemmer overens med det, der er implementeret.

UL2900-1-standarden er ikke nødvendigvis mere omfangsrig end ETSI EN 303 645, men den kræver, at man har styr på at udarbejde en god risikovurdering, hvilket kan være svært.

IEC 62443-standarden kan virke voldsom i sit omfang, men fordi den er rimelig velstruktureret, kan den for nogle være lettere at gå til end UL2900-1. Hvis man ikke har behov for at leve fuldt ud op til standarden, kan man nøjes med at se på IEC 62443-4-2, så længe man er klar over, at det mindsker meget af det underbyggende arbejde, der er med til at øge tiltroen til kvaliteten af implementeringen. Der findes desuden flere certificeringsordninger inden for IEC 62443, så det er relativt let at få nogle eksterne til at validere det arbejde, man har lavet, hvis der skulle være behov for det.

Vælg standard ud fra kravene

I det store hele drejer valget af cybersikkerhedsstandard sig om, hvilke behov, der skal dækkes. De tekniske krav i standarderne er langt hen ad vejen identiske, når der er tale om basal sikkerhed. Ofte vil det være krav fra marke-det, der dikterer, om en bestemt standard skal overholdes, eller om man kan vælge mere frit.

Det vil sjældent være spildt arbejde at udskifte den standard, der ligger til grund for, hvordan man laver sikkerhed, hvis det skulle være nødvendigt, da meget af den læring, der kommer igennem arbejdet med standarder, ikke vil ændre sig - det er blot dokumentationen og muligvis yderligere test der vil ændre sig mest.

Opsummering

Kortfattet vil anbefalingen være at benytte ETSI EN 303 645, hvis cybersikkerhed er et nyt emne, der skal håndte-res. Hvis der er et større behov for tiltro til implementering af cybersikkerhed i ens IoT-produkt, vil UL2900-1 være det oplagte valg. Hvis man derimod laver IoT-systemer til industrielle miljøer, er det IEC62443, man bør kigge på.

Kontakt
Jeppe Pilgaard Bjerre
Specialist, IoT and cyber security
Product Compliance, FORCE Technology
jpbj@force.dk
Tlf. 43 25 15 48