# IEC 62443-4-1:2018 Sikker udviklingslivscyklus for produkter inden for industriel automation

Sikker udviklingslivscyklus, otte praksisområder

47 krav. Det er muligt at blive certificeret efter denne standard hos et akkrediteret certificeringsorgan. Udgave 07/2026.

IEC 62443-4-1 kan der certificeres efter, men genstanden er usædvanlig: det, der certificeres, er udviklingsprocessen hos en navngiven udviklingsorganisation, altså en konkret dokumenteret udgave af den sikre livscyklus. Hverken et produkt eller en person bliver certificeret. Vejene er ISASecure SDLA og IECEE CB Scheme. Efter den nuværende retstilstand medfører et sådant certifikat ingen formodning om overensstemmelse med EU Cyber Resilience Act. Forveksl den ikke med IEC 62443-4-2, som stiller krav til selve komponenten. Denne liste er et arbejdsredskab til selvevaluering, ikke et bevis.

| Virksomhed | Dato | Udfyldt af |
|---|---|---|
| | | |

## 5 Praksisområde 1: Sikkerhedsstyring (SM) 13

**SM-1** **Der findes en fastlagt livscyklus for produktudvikling, som bærer sikkerheden gennem hver fase, fra den første idé til udfasning af produktet, og det er denne livscyklus, der faktisk følges i det daglige arbejde.** Dokument

Det taler for: Procesbeskrivelse eller arbejdsinstruktion, der angiver faserne, leverancerne per fase og overleveringspunkterne, sammen med dokumentation fra et igangværende projekt, der viser, at faserne reelt blev gennemarbejdet. En lille virksomhed klarer sig med en side per fase plus en tjekliste i sagssystemet; det afgørende er, at den dokumenterede proces og det daglige arbejde stemmer overens.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-2** **Hver opgave i den sikre udviklingslivscyklus har en udpeget ansvarlig, og denne fordeling er kendt af de involverede.** Dokument

Det taler for: Matrix over roller og ansvar, der kobler hvert procestrin til en navngiven rolle, suppleret med den aktuelle bemanding af rollerne. Med kun en håndfuld personer er en tabel med rolle, opgave og person tilstrækkelig; det vigtige er stedfortræderordningen ved ferie og sygdom.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-3** **Det er sporbart fastlagt, hvilke produkter, varianter, frigivelser og komponenter der er omfattet af den sikre udviklingslivscyklus, og hvilke der ikke er.** Dokument

Det taler for: Liste over de omfattede produkter og versionstilstande med en begrundelse for, hvad der regnes med, og hvad der holdes udenfor, vedligeholdt ved hver ny frigivelse. I praksis fungerer en kolonne i produktoversigten godt, med ja eller nej per række plus en sætning som begrundelse.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-4** **De personer, der påtager sig sikkerhedsopgaver, har den faglige kompetence, opgaverne kræver, og kompetencen opbygges og holdes aktuel på en bevidst måde.**

Det taler for: Kompetenceprofil per sikkerhedsrolle, registreringer over kvalifikationer, uddannelsesplan og registreringer over deltagelse, suppleret med en oversigt over hullerne. Små virksomheder dokumenterer dette med kursusbeviser, deltagelse i konferencer eller webinarer og en kort årlig gennemgang af, hvem der lukker hvilket hul hvornår, og køber ekstern ekspertise ind, hvor det er nødvendigt.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-5** **Anvendelsesområdet for den sikre udviklingslivscyklus er afgrænset og angiver de lokationer, organisatoriske enheder, leverandørbidrag og udviklingsmiljøer, der indgår, sammen med grænserne for anvendelsesområdet.** Dokument

Det taler for: Beskrivelse af anvendelsesområdet, der dækker lokationer, teams, outsourcede dele og systemer, plus en skitse over de eksterne grænseflader. Den, der udvikler på en enkelt lokation, dokumenterer dette i nogle få sætninger og nævner udtrykkeligt, hvad der ligger udenfor, for eksempel eksternt udviklede moduler eller hosting hos tredjepart.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-6** **For hvert element, der leveres til brugerne, altså software, firmware, konfigurationer og medfølgende filer, er en integritetskontrol mulig, så modtagerne kan opdage en ubemærket ændring.**

Det taler for: Signaturer eller offentliggjorte kontrolsummer per leverancepakke, en beskrivelse af metoden og et eksempel fra en reel frigivelse, sammen med en vejledning til kunden i, hvordan kontrollen udføres. For små teams er en signeret kontrolsumfil ved siden af downloadet plus et afsnit i frigivelsesnoterne nok.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-7** **Udviklings-, bygge- og testmiljøerne er beskyttet mod uautoriseret adgang og mod manipulation af kildekode, byggeværktøjer og artefakter.**

Det taler for: Koncept for adgangsstyring til repositoriet, byggeserveren og testsystemerne, adgangslister med datoen for den seneste gennemgang, registreringer af sikkerhedsrelevante ændringer og dokumentation for, at adgang til drift og udvikling er adskilt. Uden en intern IT-afdeling rækker tofaktorlogin, en beskyttet hovedgren med obligatorisk gennemgang og en gennemgang hvert halve år af, hvem der stadig har adgang.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-8** **Private nøgler, der bruges til at signere leverancer, er beskyttet mod videregivelse og misbrug, og brugen af dem er begrænset til autoriserede personer og systemer.**

Det taler for: Beskrivelse af opbevaring, adgang, fornyelse og tilbagekaldelse af nøgler, dokumentation for beskyttet opbevaring, for eksempel et hardwaretoken eller en nøglestyringstjeneste, plus registreringer af signeringerne. En lille virksomhed opbevarer signeringsnøglen på et hardwaretoken, dokumenterer de to personer med adgang og har en procedure klar til tabssituationen.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-9** **For indkøbte eller overtagne komponenter, herunder open source-software, er sikkerhedsforventningerne til leverandøren fastlagt, og de anvendes ved udvælgelsen.** Dokument

Det taler for: Sikkerhedskrav i leverandørspecifikationer eller kontrakter, udvælgelseskriterier for tredjepartskomponenter, en fortegnelse over alle tredjepartskomponenter med version og kilde, plus vurderingen af, om leverandøren opfylder forventningerne. Uden en indkøbsafdeling er en vedligeholdt komponentliste tilstrækkelig, når den har en kolonne, der viser, om leverandørens sikkerhedsopdateringer og indberetningskanaler er kontrolleret.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-10** **Komponenter, som en tredjepart udvikler på bestilling, er underlagt de samme sikkerhedskrav som intern udvikling, og overholdelsen verificeres.**

Det taler for: Indkøbsordre eller kontraktdokumenter, der angiver de krævede sikkerhedsforpligtelser, dokumentation fra leverandøren om de anvendte arbejdsmåder, registreringer fra godkendelsen og resultater af virksomhedens egne kontroller af det leverede. Uden budget til audit rækker et kontraktligt tilsagn, fremsendelse af leverandørens testresultater og en enkelt egen stikprøve inden godkendelsen.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-11** **Sikkerhedsrelevante fund fra alle kilder, altså test, gennemgange, brugerindberetninger og meddelelser fra tredjepart, registreres, vurderes for deres konsekvens, tildeles en ansvarlig og en frist og følges til afslutning.** Dokument

Det taler for: Fejl- eller sagssystem med en særlig markering af sikkerhedsemner, og per post vurderingen af konsekvensen, den ansvarlige, fristen og afslutningsnotatet, plus en oversigt over åbne punkter. Et lille team bruger en mærkat i det eksisterende sagssystem og et fast punkt på dagsordenen til ugemødet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-12** **Inden et produkt frigives, verificeres og dokumenteres det, at de planlagte trin i den sikre udviklingslivscyklus faktisk blev gennemført, og at de tilhørende registreringer blev udarbejdet.** Dokument

Det taler for: Frigivelsesgennemgang per frigivelse holdt op mod procestrinnene, henvisninger til de enkelte registreringer og en dokumenteret frigivelsesbeslutning med dato og underskrift. I praksis fungerer en frigivelsestjekliste godt, som ikke tillader forsendelse uden fuldstændige flueben; åbne punkter begrundes og får en dato.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SM-13** **Den sikre udviklingslivscyklus bliver selv regelmæssigt udfordret og forbedret ud fra erfaringer fra hændelser, testresultater, kundetilbagemeldinger og trusselsbilledet.**

Det taler for: Registreringer fra gennemgangen af processen, for eksempel ledelsens evaluering eller et tilbageblik, med de procesændringer den udløste, deres gennemførelsesstatus og en henvisning til grundårsagen. Den, der bruger standardens modenhedsniveauer, registrerer den aktuelle tilstand og målet per praksisområde; modenhedsniveau 4 kræver netop denne dokumentation for løbende forbedring. For en lille virksomhed er et møde om året med referat og tre konkrete forbedringer nok.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 6 Praksisområde 2: Specifikation af sikkerhedskrav (SR) 5

**SR-1** **Den tilsigtede produktkontekst er beskrevet: forventet driftsmiljø, de sikkerhedsforanstaltninger, der forudsættes leveret af dette miljø, tilsigtede brugergrupper og roller, antagne tillidsgrænser og de anvendelser, som produktet udtrykkeligt ikke er beregnet til.** Dokument

Det taler for: En beskrivelse af produktets sikkerhedskontekst, enten som et selvstændigt dokument eller som et fast afsnit i produktspecifikationen, der dækker netværksmiljøet, de antagne eksterne beskyttelser, for eksempel en firewall eller fysisk adgangsstyring, en liste over roller og en udtrykkelig liste over anvendelser uden for anvendelsesområdet. En lille virksomhed holder dette på to sider, tilføjer en enkel skitse af anlægsmiljøet og lader produktejeren datere og godkende det.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SR-2** **Der findes en trusselsmodel for produktet, som kortlægger datastrømme, grænseflader, tillidsgrænser og angrebsveje, navngiver de trusler, der følger heraf, og deres mulige konsekvens, og tildeler modforanstaltninger. Den gennemgås og opdateres ved relevante ændringer og mindst en gang per produktfrigivelse, og åbne punkter følges, indtil de er lukket.** Dokument

Det taler for: Trusselsmodel med et dataflowdiagram, en trusselsliste per grænseflade, tildelte modforanstaltninger og status på åbne punkter, plus en revisionshistorik med dato og forfatter. En lille virksomhed kan arbejde ud fra en tabel per grænseflade med kolonner for, hvad der kan gå galt der, hvor slemt det ville være, hvad der gøres ved det, og hvem der gennemgår det.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SR-3** **Sikkerhedskravene til produktet er fastlagt og dokumenteret. De dækker resultaterne af trusselsmodellen, den beskrevne sikkerhedskontekst for produktet, gældende juridiske og kontraktlige forpligtelser og det tilstræbte sikkerhedsniveau, og de omfatter de sikkerhedsfunktioner, produktet selv skal levere.** Dokument

Det taler for: Kravliste eller værktøj til kravstyring med en entydig identifikator per krav, kilden til hver post, for eksempel en trussel, en kundekontrakt eller en juridisk forpligtelse, og det tilstræbte sikkerhedsniveau. En lille virksomhed kører dette som en enkelt tabel med en fast ID-kolonne, som verifikation og test senere kobler sig på.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SR-4** **Hvert enkelt sikkerhedskrav er formuleret, så det er entydigt, uden modsigelser, testbart og sporbart til en bestemt produktfunktion eller grænseflade, og det bærer de oplysninger, der senere skal bruges til at verificere det uden yderligere afklaring.**

Det taler for: En stikprøve fra kravlisten, der for hvert krav viser et målbart acceptkriterium og den berørte funktion eller grænseflade, sammen med koblingen mellem krav og testtilfælde. En lille virksomhed kontrollerer dette med en fast formuleringsskabelon og kontrolspørgsmålet, om der kan skrives et testtilfælde ud fra kravet uden at spørge tilbage.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SR-5** **Sikkerhedskravene gennemgås, inden de bruges i design og implementering, med inddragelse af de berørte parter, for eksempel udvikling, test, produktejerskab og, hvor det er nyttigt, salg eller kunden. Gennemgangen dækker fuldstændighed i forhold til trusselsmodellen og produktets sikkerhedskontekst, korrekthed og testbarhed. Fund registreres og følges til afslutning.**

Det taler for: Registrering fra gennemgangen med dato, deltagere og deres roller, den gennemgåede version af kravene, en liste over fund med en ansvarlig og afslutningsstatus samt et godkendelsesnotat. En lille virksomhed håndterer dette som en gennemgang mellem to personer fra udvikling og test, med en kort registrering og en godkendelseslinje i kravlisten.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 7 Praksisområde 3: Sikkerhed indbygget i designet (SD) 4

**SD-1** **Hvert produkt har en designbeskrivelse, der fastholder de sikkerhedsrelevante dele af arkitekturen: hvilke komponenter der findes, hvordan de kommunikerer indbyrdes, hvor tillidsgrænserne går, hvilke eksterne grænseflader der er eksponeret, og med hvilke mekanismer de tidligere fastlagte sikkerhedskrav realiseres i designet.** Dokument

Det taler for: Arkitekturdokument eller designspecifikation med et diagram, der viser komponenter, datastrømme og tillidsgrænser, plus en koblingstabel fra hvert sikkerhedskrav til det designelement, der realiserer det. En lille leverandør klarer sig med et vedligeholdt diagram plus to eller tre siders forklaring; det afgørende er, at det er versionsstyret i repositoriet og opdateres, hver gang arkitekturen ændres.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SD-2** **Designet analyseres systematisk for trusler. Analysen navngiver angriberes mål, de berørte tillidsgrænser og grænseflader, de trusler, der følger heraf, sammen med deres vurdering, og de modforanstaltninger, der er truffet i designet. Den gentages, hver gang arkitektur eller miljø ændres væsentligt, og identificerede trusler følges, indtil der er truffet en beslutning om hver enkelt.** Dokument

Det taler for: Trusselsmodel per produkt eller per større frigivelse, for eksempel en tabel med kolonner for trussel, berørt grænseflade, vurdering, modforanstaltning og status, sammen med referatet fra modelleringsmødet med deltagere og dato. Et lille team modellerer pragmatisk i en workshop på to til tre timer langs arkitekturdiagrammet og noterer åbne punkter som sager, så dokumentationen for opfølgningen opstår uden ekstra arbejde.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SD-3** **Designet følger påviseligt anerkendte principper for sikkert design, blandt andet færrest mulige rettigheder, mindst mulig angrebsflade, forsvar i dybden, sikre standardindstillinger, sikker tilstand ved fejl og sikkerhedsmekanismer, der er så enkle og verificerbare som muligt. Anvendelsen af disse principper er synlig i designet og begrundet.**

Det taler for: Et afsnit i designbeskrivelsen eller en intern designretningslinje, der navngiver principperne, plus konkret dokumentation per princip i produktet, for eksempel rettighedsmatrixen for tjenesterne, listen over åbne porte med begrundelse, standardindstillingerne ved levering eller den dokumenterede fejlhåndtering. En lille leverandør bruger en kort tjekliste over disse principper som fast punkt i designgennemgangen og arkiverer det udfyldte skema sammen med designet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SD-4** **Designet gennemgås af kvalificerede fagfæller, inden implementeringen begynder. Gennemgangen dækker fuldstændighed i forhold til sikkerhedskravene, korrektheden og virkningen af sikkerhedsmekanismerne og resultaterne af trusselsanalysen. Personer med tilstrækkelig sikkerhedskompetence deltager, fund registreres og følges til afslutning.** Dokument

Det taler for: Registrering fra gennemgangen med dato, den gennemgåede genstand med angivelse af version, deltagere og deres roller, liste over fund med status og frigivelsesbeslutningen. Et lille team hænger gennemgangen på pull requesten til designdokumenterne og efterlader fundene som kommentarer med et afslutningsnotat, hvilket dokumenterer opfølgningen uden yderligere værktøjer. Mangler sikkerhedskompetencen internt, er en ekstern fagperson hyret på timebasis til de kritiske design den pragmatiske vej.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 8 Praksisområde 4: Sikker implementering (SI) 2

**SI-1** **Der findes en fastlagt proces for at verificere den faktiske implementering op mod det sikre design: gennemgangen bekræfter, at de beskyttelsesforanstaltninger, designet forudser, reelt findes og er virksomme i koden, at forsvar i dybden er bevaret, og at der ikke er indført nye sårbarheder under implementeringen. Gennemgangen udføres af passende kvalificeret personale, og fundne afvigelser registreres og følges til afslutning.**

Det taler for: En skriftlig procedure for gennemgang af implementeringen sammen med registreringer per komponent eller frigivelse: det gennemgåede modul, henvisningen til designdokumentet, datoen, den ansvarlige for gennemgangen, fundene og deres afklaringsstatus. Egnet dokumentation er blandt andet gennemgange i pull requests med en obligatorisk sikkerhedstjekliste, resultater af statisk kodeanalyse med en dokumenteret vurdering af hvert træf og referater fra gennemgangsmøder. Et lille team dækker dette med fireøjneprincippet, en gennemgangsskabelon i repositoriet, hvor hver designforanstaltning afkrydses enkeltvis, og en sag per åbent fund. Det afgørende er, at den, der har skrevet koden, aldrig er den, der gennemgår netop den kode.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SI-2** **Bindende regler for sikker kodning gælder for alt sikkerhedsrelevant udviklingsarbejde og dækker som minimum undgåelse af kendte usikre konstruktioner og funktioner, håndteringen af input og fejl, styringen af hukommelse og ressourcer og brugen af afprøvet sikkerhedskode frem for selvskrevne implementeringer. Reglerne gælder per anvendt programmeringssprog, er kendt af alle udviklere og opdateres, når der er behov, for eksempel når nye angrebsmønstre eller nye værktøjer dukker op.** Dokument

Det taler for: En godkendt standard for sikker kodning med versionsstatus, anvendelsesområde per sprog og godkendelsesdato, suppleret med dokumentation for, at den virker i det daglige arbejde: konfigurationen af lintere og analyseværktøjer i repositoriet, en byggeregel, der synliggør overtrædelser, og deltagerlisten fra orienteringen. Små virksomheder skriver ikke en standard fra bunden; de gør et etableret offentligt regelsæt bindende, tilføjer en kort liste over egne supplerende regler og forankrer kontrollen i pipelinen, så overholdelsen påvises automatisk.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 9 Praksisområde 5: Test til verifikation og validering af sikkerheden (SVV) 5

**SVV-1** **Hvert sikkerhedsrelevant produktkrav har mindst et testtilfælde tilknyttet, som viser, at beskyttelsesfunktionen virker som tilsigtet i normal drift, at den opfører sig som specificeret ved ugyldigt input eller misbrug, og at de standardindstillinger, produktet leveres med, svarer til den sikre tilstand. Udførelse og resultat registreres for hver testet softwareversion.**

Dokument

Det taler for: En sporbarhedsmatrix, der forbinder krav med testtilfælde og resultat, plus testregistreringer med dato, den testede version eller det testede build og navnet på den, der udførte testen. En lille leverandør tilføjer blot en kolonne med testtilfældets ID i kravlisten og arkiverer logudskriften fra den automatiske testkørsel i byggepipelinen som en fil knyttet til den pågældende version.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

**SVV-2** **De modforanstaltninger, der stammer fra trusselsmodellen, testes målrettet for at bekræfte, at de faktisk lukker den antagne angrebsvej. Der testes mod de identificerede trusler, ikke kun mod forventet, korrekt brug, og åbne punkter føres ind i fejlhåndteringsprocessen.**

Det taler for: Testtilfælde, der henviser direkte til posterne i trusselsmodellen, for eksempel et misbrugsscenarie per trussels-ID med den forventede forsvarsadfærd, sammen med registreringerne fra kørslerne. Uden tungt maskineri rækker det at tilføje en kolonne i trusselsmodellen med henvisning til testtilfældet og datoen for den seneste vellykkede kontrol.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

**SVV-3** **Produktet undersøges systematisk for sårbarheder inden frigivelsen. Omfanget dækker som minimum: undersøgelse af de eksternt tilgængelige grænseflader og tjenester, test med fejlformet og tilfældigt muteret input, gennemgang af de anvendte tredjepartskomponenter op mod kendte indberettede sårbarheder og en kontrol for kendte svaghedsklasser i leverandørens egen kode. Fund registreres sammen med deres vurdering.**

Dokument

Det taler for: Rapporter fra de anvendte værktøjer med værktøjets navn, version og datastatus for sårbarhedsdatabasen, registreringer fra fuzzing, en liste over tredjepartskomponenter med datoen for den seneste sammenligning og listen over fund med vurdering og beslutning. En lille leverandør kombinerer gratis standardværktøjer, en afhængighedsscanning og en scanning af porte og tjenester mod det installerede produkt og lægger resultaterne per frigivelse i en enkelt mappe.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

**SVV-4** **Frigivelseskandidaten udsættes for et angrebsforsøg under realistiske forhold, som aktivt forsøger at omgå beskyttelsesmekanismerne i stedet for blot at afprøve dem. Omfang, rammebetingelser og grænser for testen aftales på forhånd, og de fundne svagheder håndteres og følges som fejl.**

Det taler for: Aftalen eller testordren med angivelse af omfang og testmiljø, en rapport om fremgangsmåden, de udnyttede svagheder og deres vurdering, plus posterne i fejl- eller sagssystemet med dokumentation for udbedring eller for en begrundet risikoaccept. Små leverandører køber typisk denne test eksternt inden for et afgrænset tidsbudget eller lader den udføre af en person, der ikke har udviklet produktet.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

**SVV-5** **Testpersonalets uafhængighed er fastlagt og passer til det tilstræbte modenhedsniveau. Den, der har udviklet en komponent, frigiver den ikke alene på grundlag af sin egen test, og efterhånden som modenhedsniveauet stiger, ligger testen hos en organisatorisk adskilt enhed eller en ekstern part. Den faktiske fordeling er sporbar for hver test.**

Det taler for: En rollebeskrivelse i udviklingsprocessen, der viser adskillelsen af udvikling og test, plus for hver testkørsel eller testrapport det registrerede navn og den registrerede rolle på den, der udførte testen. En virksomhed med to personer håndterer dette med gensidig gennemgang og et dokumenteret notat om fireøjneprincippet og henter en ekstern person ind til den dybdegående sikkerhedstest.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

## 10 Praksisområde 6: Håndtering af sikkerhedsfejl (DM) 6

**DM-1** **Der findes en fastlagt kanal, hvor indberetninger om sikkerhedssvagheder i produktet modtages og registreres fra alle retninger: fra udviklingsteamet selv, fra test og gennemgange, fra kunder og integratorer, fra eksterne indberettere og fra sikkerhedsmeddelelser om anvendte tredjepartskomponenter og open source-komponenter. Indberetningskanalen kan findes af eksterne parter, og hver indberetning registreres med modtagelsesdato og kilde.** Dokument

Det taler for: En beskrivelse af indberetningskanalen, det offentligt tilgængelige kontaktpunkt (en sikkerhedsside, en security.txt-fil eller en postkasse som security@) og modtageregistret med dato, kilde og en kort beskrivelse for hver indberetning. En lille virksomhed kan klare sig med en fælles postkasse og et enkelt regneark eller en mærkat i sagssystemet, så længe hver indberetning ender der, også dem, der rejses i den interne udviklerchat.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**DM-2** **Hver indkommen indberetning visiteres og undersøges for at afgøre, om den er sikkerhedsrelevant, og hvilke produkter, versioner og komponenter den berører. Indberetninger, der viser sig ikke at være sikkerhedsrelevante eller ikke at gælde, lukkes også med en angivet begrundelse i stedet for at blive kasseret i stilhed.**

Det taler for: Et visiteringsnotat for hver indberetning med resultatet (sikkerhedsrelevant ja eller nej), de berørte versioner og begrundelsen for afvisning, hvor det er relevant, synligt i sagen eller i modtagelisten. Teams med få indberetninger kan gennemføre visiteringen i et kort tilbagevendende møde og notere resultatet i to sætninger per post.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**DM-3** **Bekræftede sikkerhedsfejl vurderes efter en ensartet metode: grundårsag, berørte versioner og konfigurationer, mulig konsekvens for drift og sikkerhed, udnyttelighed og alvorlighed efter en fastlagt skala. Resultatet af vurderingen registreres og er sporbart.** Dokument

Det taler for: En vurderingsregistrering eller et sæt sagsfelter for hver fejl, der dækker grundårsag, alvorlighed og den anvendte skala (for eksempel et udbredt system til vurdering af alvorlighed med en dokumenteret vektor), sammen med listen over berørte versioner. Små teams kan nøjes med en fast feltskabelon i sagssystemet plus en halv side, der beskriver skalaen og de tærskler, der udløser omgående handling.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**DM-4** **For hver vurderet sikkerhedsfejl træffes der en beslutning om håndteringen: udbedring, kompenserende foranstaltning eller en begrundet accept af risikoen. Beslutningen følger af alvorligheden, den tildeles en ansvarlig person og en frist, og fejlen følges til afslutning.** Dokument

Det taler for: En handlingsliste eller sagsstatus med ansvarlig, måldato, foranstaltningstype og et afslutningsnotat, koblet til den kodebaseline eller den frigivelse, hvor rettelsen får virkning. Accepterede restrisici kræver en kort skriftlig begrundelse, som produktejerskabet godkender. En lille virksomhed kan holde dette i en sagstavle med frister, uden yderligere værktøjer.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**DM-5** **Berørte brugere, integratorer og andre interessenter informeres om sikkerhedsfejl, så snart vurderingen tilsiger det, med angivelse af de berørte versioner, konsekvensen og den tilgængelige rettelse eller kompenserende foranstaltning. Frister og modtagerkredsen for en sådan offentliggørelse er fastlagt på forhånd, og det samme gælder fremgangsmåden ved indberetninger fra tredjepart, der selv har en frist for offentliggørelse.**

Det taler for: Offentliggjorte sikkerhedsmeddelelser med dato og versionshenvisning, distributionslisten eller abonnementskanalen og den skriftlige regel om frister og koordineret offentliggørelse. Leverandører med få kunder kan bruge en enkelt udsendelse til en vedligeholdt kundeliste plus en dateret side med sikkerhedsmeddelelser, hvis ændringer er versionsstyrede.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**DM-6** **Håndteringen af sikkerhedsfejl gennemgås med faste intervaller. Gennemgangen ser på åbne og overskredne sager, tiden fra indberetning til udbedring, tilbagevendende grundårsager og virkningen af de trufne foranstaltninger. Forbedringer af processen, der følger af gennemgangen, gennemføres, og gennemførelsen følges.** Dokument

Det taler for: Referat fra den tilbagevendende gennemgang med dato, deltagere, tal for åbne og overskredne sager og en liste over aftalte forbedringer med ansvarlig og frist. En lille virksomhed kan hænge dette punkt på et eksisterende kvartalsmøde og holde tallene og beslutningerne på en enkelt side.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 11 Praksisområde 7: Håndtering af sikkerhedsopdateringer (SUM) 5

**SUM-1** **Hver sikkerhedsopdatering til produktet verificeres mod de understøttede produktversioner og driftsmiljøer, inden den frigives til kunderne, og der findes en registrering, der viser, at opdateringen lukker sårbarheden uden at forstyrre den tilsigtede produktfunktion.** Dokument

Det taler for: Testregistrering per rettelse med den testede produktversion, platformen, testtilfældene (virkning mod sårbarheden plus regression af kernefunktionerne) og frigivelsesgodkendelsen. En lille leverandør kan klare sig med en kort godkendelsespost for rettelsen i sagen: sagsnummer, verificeret af, verificeret den, resultat, med loggen fra den automatiske testkørsel vedhæftet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SUM-2** **For alle produktkomponenter, der ikke er udviklet internt (tredjepartsbiblioteker, operativsystem, runtimemiljøer), er det fastlagt og dokumenteret, hvordan deres sikkerhedsopdateringer vurderes og enten optages i produktet eller afvises med en dokumenteret begrundelse.** Dokument

Det taler for: Komponentfortegnelse over tredjepartsdelene med version og kilde, plus en vurderingspost per indberettet sårbarhed i tredjepart med beslutningen (optages, ikke berørt, dækket af en kompenserende foranstaltning) og begrundelsen. Små teams kører en automatisk afhængighedsscanning i byggeprocessen og holder beslutningerne som kommentarer til scanningsresultatet eller i en slank undtagelsesliste.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SUM-3** **For hver sikkerhedsopdatering, der udsendes, får brugerne forståelig ledsagende information: hvilke produktversioner der er berørt, hvilken sårbarhed der er rettet, hvor alvorlig den er, om der skal tages hensyn til bivirkninger eller kompenserende foranstaltninger, og hvordan opdateringen installeres.** Dokument

Det taler for: Offentliggjorte sikkerhedsmeddelelser eller frigivelsesnoter med sårbarhedens identifikator, de berørte versioner, vurderingen af alvorligheden, installationstrinnene og vejledning i at rulle tilbage til den tidligere tilstand. Små leverandører holder en enkelt offentlig side med en kronologisk liste over sikkerhedsmeddelelser og henviser til den inde fra produktet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SUM-4** **Der findes en fastlagt og manipulationsbeskyttet vej, ad hvilken brugerne henter sikkerhedsopdateringer, og en opdaterings ægthed og integritet kan verificeres hos brugeren, inden den installeres.**

Det taler for: Beskrivelse af leveringskanalen (downloadområde, opdateringsserver, fysiske medier) sammen med dens beskyttelsesforanstaltninger, plus den digitale signatur eller kontrolsum per pakke og en vejledning, der fortæller brugeren, hvordan den verificeres. Små leverandører opnår dette ved at signere på byggeserveren, offentliggøre kontrolsummen ved siden af downloadet og angive et entydigt sted, hvor den offentlige nøgle ligger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SUM-5** **Der findes fastlagte tidsmål for, hvornår sikkerhedsopdateringer stilles til rådighed, gradueret efter sårbarhedens alvorlighed; de faktisk opnåede tider følges, og et tidsmål, der overskrides, begrundes og understøttes af en midlertidig foranstaltning for brugerne.** Dokument

Det taler for: Intern specifikation med et tidsvindue per alvorlighedskategori (for eksempel kritisk <= 30 dage, høj <= 90 dage) og en opgørelse per sårbarhed: indberetningsdato, dato for frigivelse af rettelsen, forløbne dage, årsag til afvigelsen. Små leverandører holder dette som to datofelter i sårbarhedssagen og gennemgår listen en gang i kvartalet i stedet for at opbygge et særskilt målesystem.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

## 12 Praksisområde 8: Sikkerhedsvejledninger til idriftsættelse og drift af produktet (SG) 7

**SG-1** **Hvert produkt leveres med en beskrivelse af sin strategi for forsvar i dybden: den navngiver de beskyttelseslag, der er indbygget i selve produktet, kobler dem til de trusler, de imødegår, og viser, hvilken beskyttende virkning der først opstår i samspillet mellem flere lag.** Dokument

Det taler for: Et afsnit i den leverede produktdokumentation eller et selvstændigt sikkerhedskoncept, der for hvert beskyttelseslag angiver mekanismen, den dækkede trussel og grænserne for virkningen. En lille virksomhed holder dette som en tabel på to sider: kolonne beskyttelseslag, kolonne trussel hentet fra virksomhedens egen trusselsmodel, kolonne restrisiko. En krydshenvisning til trusselsmodellen fra SR-2 er tilstrækkelig, indholdet behøver ikke at blive vedligeholdt to gange.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-2** **Dokumentationen navngiver de sikkerhedsforanstaltninger, produktet ikke selv leverer, men forventer af driftsmiljøet, for eksempel netværkssegmentering, foranstillede firewalls, fysisk adgangsstyring eller en ekstern tidstjeneste, og gør det klart, at det lovede sikkerhedsniveau ikke nås uden disse foranstaltninger.** Dokument

Det taler for: Et kapitel om forudsætninger for idriftsættelse i manualen eller en referencearkitekturtegning med zoner og forbindelser, hvor de foranstaltninger, anlægsejeren skal levere, er udtrykkeligt markeret. En liste over antagelser om miljøet har vist sig nyttig i praksis, afledt direkte af produktets sikkerhedskontekst og gennemlæst igen ved hver produktversion.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-3** **Der findes en vejledning til sikker basiskonfiguration, som lister alle sikkerhedsrelevante indstillinger, tjenester, porte og grænseflader, angiver den anbefalede tilstand ved levering og beskriver konsekvensen af at afvige fra anbefalingen.** Dokument

Det taler for: Hærdningsvejledning med en tabel over indstillinger: parameter, anbefalet værdi, virkning, bivirkning ved afvigelse. Plus listen over de tjenester og porte, der er aktive i standardkonfigurationen, med en begrundelse for, hvorfor de forbliver slået til. Et lille team holder denne tabel lige ved siden af konfigurationsfilen i repositoriet og eksporterer den til leverancedokumentationen, så den følger produktet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-4** **Til den løbende drift findes en vejledning, der beskriver, hvordan produktet drives sikkert, overvåges og holdes i sin sikre tilstand, herunder sikkerhedskopiering og genetablering, logning og håndteringen af sikkerhedsrelevante hændelsesmeddelelser.** Dokument

Det taler for: Driftsvejledning med afsnit om logning, sikkerhedskopier, genstart og hændelsesmeddelelser. Som yderligere dokumentation en liste over de sikkerhedsrelevante meddelelser, produktet udsender, hver med en kort anbefalet handling, så anlægsejeren ikke behøver at tolke dem alene.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-5** **Dokumentationen forklarer, hvordan produktets brugerkonti, roller og rettigheder oprettes og vedligeholdes, især adskillelse af roller, ændring af standardadgangsoplysninger og fjernelse af konti, der ikke længere er nødvendige.** Dokument

Det taler for: Et kapitel om kontostyring med en oversigt over roller og de rettigheder, hver rolle har, plus en udtrykkelig bemærkning om standardadgangsoplysninger og om at ændre dem ved idriftsættelsen. En kort tjekliste til idriftsættelsen i manualen fungerer godt i praksis, en, som anlægsejeren kan krydse af og arkivere.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-6** **Der findes en vejledning til sikker udfasning, som beskriver den fuldstændige fjernelse af følsomme data fra produktet, for eksempel adgangsoplysninger, nøgler, konfigurationsdata og logfiler, inden enheden gives videre, genbruges eller bortskaffes.** Dokument

Det taler for: Et afsnit om udfasning, der lister hvert lagringssted for følsomme data inde i produktet og den tilhørende sletteprocedure, herunder de tilfælde, hvor sletning er teknisk umulig, og hardwaren skal destrueres fysisk. En liste over vedvarende lagre hentet fra arkitekturbeskrivelsen hjælper her, den forhindrer, at et lagringssted bliver glemt.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

**SG-7** **Den sikkerhedsdokumentation, der leveres til brugerne, gennemgås inden frigivelsen: den er teknisk korrekt, i overensstemmelse med den leverede produktversion, fuldstændig i forhold til det tilsigtede indhold og forståelig for den tilsigtede målgruppe, og den opdateres, hver gang produktet ændres.**

Det taler for: En registrering fra gennemgangen per dokument og produktversion med den ansvarlige for gennemgangen, dato, fund og deres afslutning, koblet til frigivelsesgodkendelsen. En lille virksomhed løser dette med fireøjneprincippet i pull requesten til dokumentationen: en udvikler kontrollerer det tekniske indhold, en anden person kontrollerer forståeligheden, og godkendelsen registreres i sagen. En version kan først sendes ud, når gennemgangen er dokumenteret.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse