Cyberklar 2025:

Alt du skal vide om EU's nye lovkrav for embedded elektronik

engineer minds
we bring qualified people

Indhold

Hvorfor er cybersikkerhed kritisk nu mere end nogensinde?

Cybertruslerne vokser, og EU har skærpet kravene med **Cyber Resilience Act (CRA) og Radio Equipment Directive – Delegated Act (REDDA)**. Begge er nu endeligt godkendt – REDDA er allerede under implementering, mens CRA træder i kraft i december 2024 med en overgangsperiode frem til 2027.

For virksomheder, der udvikler elektronik med digitale elementer – alt fra indlejrede systemer og softwarekomponenter til netværksforbundne enheder – betyder det, at sikkerhed ikke længere er noget, man kan vælge til – det er en nødvendighed. Formålet med CRA er at beskytte forbrugere og styrke Unionens overordnede modstandsdygtighed ved at gøre digitale produkter mere sikre. Dette indebærer at reducere risici for både private brugere og vigtige enheder som hospitaler og banker.

Hvis du udvikler elektronik, er det ikke længere et spørgsmål om "hvis", men om "hvordan" du sikrer, at dine produkter lever op til kravene. CRA har en defensiv tilgang til cybersikkerhed, hvor fokus er på at beskytte produkter mod potentielle trusler.

Når virksomheden skal gennemgås for cybersikkerhed, kan det ofte betale sig at kombinere det med forbedring af kvalitet og optimering af processer.
Det er vigtigt, at ledelsen er involveret og støtter processen mod bedre cybersikkerhed.

Denne e-bog giver dig en praktisk guide til at forstå reglerne, og vigtigst af alt: hvordan du konkret kommer i mål med at implementere datasikkerhed i din udvikling.

Per Timo Kragh

Managing Partner
+45 29 605 405
per@engineerminds.dk

engineer minds
we bring qualified people

Den kommende EU-regulering – hvad betyder den for dig?

Hovedpunkter i CRA og REDDA

EU har med Cyber Resilience Act (CRA) og Radio Equipment Directive – Delegated Act (REDDA) indført nye standarder for cybersikkerhed i digitale produkter. Lovgivningen er vedtaget og trådte i kraft i december 2024 med overgangsperiode frem til 2027.

Selvom loven trådte i kraft i december 2024, er der en overgangsperiode frem til 2027 for de fleste krav. Det er dog vigtigt at bemærke, at obligatorisk indberetning af hændelser og sårbarheder træder i kraft allerede i 2026.

Loven har ét klart formål: at skabe sikre digitale produkter, der beskytter mod cybertrusler og styrker tilliden på markedet. CRA gør producenters ansvar officielt (og i visse tilfælde også importørers og distributørers) for den digitale sikkerhed af de produkter, de markedsfører. De skal tænke på - og garantere - produkternes digitale sikkerhed gennem hele deres livscyklus, fra design til ophør af support.

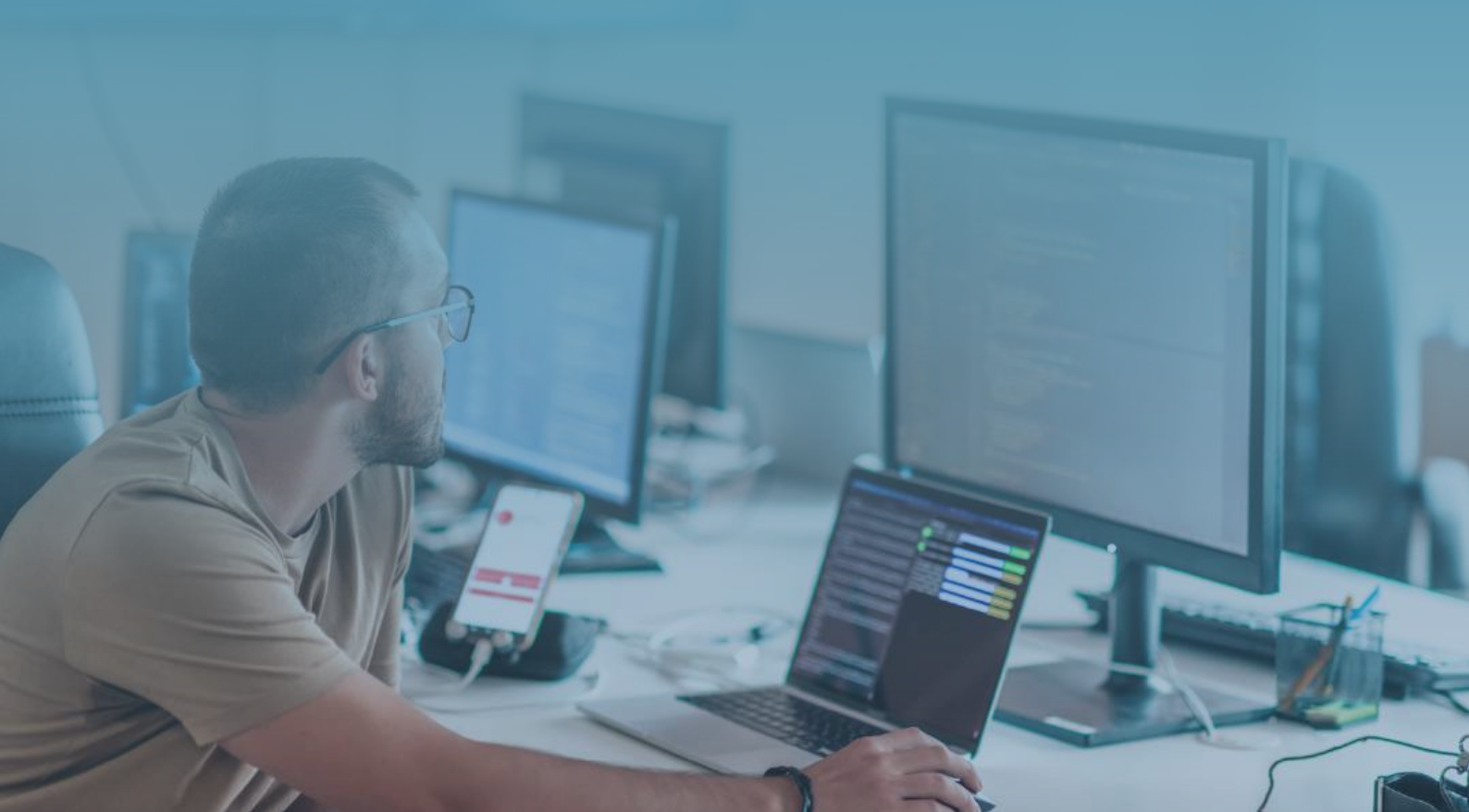
Hvem gælder lovgivningen for?

CRA og REDDA gælder bredt og omfatter:

- Producenter af digitale produkter i EU.
- Importører og distributører, der bringer produkter ind på EU-markedet.
- Udviklere af software og indlejrede systemer.
- Open Source Software (OSS) Stewards: *"Juridiske personer, der systematisk yder vedvarende support til udviklingen af specifikke produkter med digitale elementer, der kvalificerer som fri og open source-software og er beregnet til kommercielle aktiviteter, og som sikrer disse produkters levedygtighed."*
- CRA gælder ikke for fysiske eller juridiske personer, der bidrager med kildekode til produkter med digitale elementer, der kvalificerer som fri og open source-software, som ikke er under deres ansvar.

Små- og mellemstore virksomheder (SMV'er):

- SMV'er kan være underlagt forenklede procedurer for teknisk dokumentation.
- De kan være undtaget fra visse økonomiske sanktioner i forbindelse med overtrædelse af tidsfrister for indberetning af hændelser og sårbarheder.
- Reglerne stiller krav til alt fra industrielle systemer og netværksudstyr til hardware og software, så længe de indeholder digitale elementer.



Hvilke konsekvenser kan det få for virksomheder?

Den nye regulering betyder, at cybersikkerhed skal tænkes ind fra starten – security by design – og løbende vedligeholdes gennem produktets livscyklus. Manglende overholdelse kan få store konsekvenser:

- **Økonomiske sanktioner:** Høje bøder og krav om at udbedre mangler.
- **Tab af markedsadgang:** Uden compliance kan produkter ikke markedsføres i EU.
- **Omdømme og kundetillid:** Cybersikkerhedsbrud kan skade virksomhedens ry og kundernes tillid.

Risikoen ved manglende cybersikkerhed

Manglende cybersikkerhed kan få alvorlige konsekvenser – både teknisk, økonomisk og omdømmemæssigt.

Eksempler på trusler

- Hacking af kritisk infrastruktur: Cyberangreb på vindmøller, industrielle kontrolsystemer eller energinetværk kan føre til omfattende nedetid.
- Datatyveri: Hackere kan stjæle følsomme oplysninger som produktdata og kundeinformation.
- Ransomware-angreb: Virksomheder kan miste adgang til deres egne systemer, hvilket kan medføre store økonomiske tab.

Økonomiske konsekvenser

- Direkte tab: Nedetid, tabte indtægter og genoprettelsesomkostninger.
- Bøder: CRA kan pålægge virksomheder bøder på op til 15 millioner euro eller 2,5 % af den globale omsætning.
- Tabte markedsandele: Usikre produkter kan miste kundernes tillid.

Sådan forbereder din virksomhed sig på de nye cybersikkerhedskrav

Tjekliste for compliance

For at sikre compliance med CRA og REDDA skal virksomheder følge en struktureret tilgang:

- **Få styr på kravene:**
  Gennemgå de specifikke regler og deadlines. Identificér, hvilke produkter og processer der er omfattet.

- **Udfør en risikovurdering og GAP-analyse:**
  Sammenlign dine nuværende praksisser med de nye krav. Identificer trusler og sårbarheder. Risikovurderingen bør omfatte en analyse baseret på produktets tilsigtede formål, brugsbetingelser (f.eks. driftsmiljø) og forventede brugstid. Det skal også tydeligt angives, hvordan de væsentlige produktkrav gælder for det pågældende produkt, og hvordan de implementeres, hvordan producenten vil sikre, at produktet er designet, udviklet og produceret på en måde, der garanterer et passende niveau af cybersikkerhed, og hvordan producenten vil anvende de væsentlige krav til håndtering af sårbarheder. Hvis produktet integrerer tredjepartskomponenter, herunder open source-komponenter, skal der udvises "due diligence" for at vurdere risiciene.

- **Integrér sikkerhed fra starten:**
  Brug security by design-tilgangen.

(Fortsættes på næste side)

- **Planlæg sikkerhedsopdateringer:**
  Opstil procedurer for rapportering og håndtering af sårbarheder.

- **Træn dine medarbejdere:**
  Uddan dit team i de nye krav.

- **Dokumentér alt:**
  Dokumentér risikovurderinger og løsninger for at kunne demonstrere compliance. Den tekniske dokumentation skal indeholde alle oplysninger, der viser, at produktet og de processer, der er implementeret af producenten, overholder de væsentlige krav i CRA. Dette omfatter en generel beskrivelse af produktet, versioner af software, der påvirker overholdelsen af de væsentlige krav, fotografier eller illustrationer af hardwareprodukter, brugerinformation og instruktioner som angivet i Annex II i forordningen, en vurdering af de cybersikkerhedsrisici, som produktet er designet til at beskytte imod, relevant information, der er taget i betragtning for at bestemme supportperioden, en liste over de anvendte harmoniserede standarder, fælles specifikationer eller europæiske certificeringsordninger, testrapporter og en kopi af EU-overensstemmelseserklæringen.

Implementering af cybersikkerhed kan give et kvalitetsløft til din virksomhed.

Denne tabel opsummerer de vigtigste punkter fra tjeklisten, som kan hjælpe dig med at opnå dette kvalitetsløft og styrke din markedsposition.

Hent hele tabellen her

Udover at undgå bøder, kan din virksomhed opnå en stærkere markedsposition.

Harmoniserede standarder og tekniske specifikationer

For at opfylde de væsentlige krav i CRA kan europæiske harmoniserede standarder anvendes. Disse standarder er tekniske retningslinjer udarbejdet af standardiseringsorganer, og de dokumenterer, at produkter og tjenester opnår et bestemt niveau af kvalitet, sikkerhed og pålidelighed.

Et eksempel på et nyttigt dokument er "Cyber Resilience Act Requirements Standards Mapping (2024)", udgivet af Joint Research Centre (JRC) og European Union Agency for Cyber Security (ENISA). Dette dokument kortlægger hvert af CRA's væsentlige krav til en eller flere eksisterende standarder.

Rapportering af hændelser og sårbarheder

Producenter skal underrette **ENISA** (European Union Agency for Cyber Security) og nationale **CSIRT'er** (Computer Security Incident Response Teams) om alvorlige hændelser og aktivt udnyttede sårbarheder. Disse underretninger skal ske samtidigt via en "single reporting platform". En "alvorlig hændelse" er en hændelse, der negativt påvirker et produkts evne til at beskytte tilgængeligheden, autenticiteten, integriteten eller fortroligheden af følsomme eller vigtige data eller funktioner, eller som har ført til introduktion eller udførelse af ondsindet kode. En "aktivt udnyttet sårbarhed" er en sårbarhed, hvor der er pålidelig dokumentation for, at en ondsindet aktør har udnyttet den i et system uden tilladelse fra systemets ejer.

Tidsfrister for indberetning af alvorlige hændelser:

- Tidlig varsling inden for 24 timer efter at være blevet opmærksom på hændelsen.
- Anden underretning senest 72 timer efter at være blevet opmærksom på hændelsen.
- En endelig rapport senest 14 dage efter, at en korrigerende eller afhjælpende foranstaltning er blevet tilgængelig.

Tidsfrister for indberetning af aktivt udnyttede sårbarheder:

- Tidlig varsling inden for 24 timer efter at være blevet opmærksom på den.
- Anden underretning senest 72 timer efter at være blevet opmærksom på den.
- En endelig rapport senest 14 dage efter, at en korrigerende eller afhjælpende foranstaltning er blevet tilgængelig.

Coordinated Vulnerability Disclosure (CVD) politik

Det er vigtigt at implementere en CVD-politik, som omfatter en **Vulnerability Disclosure Program** (VDP). En VDP er en struktureret kanal, der giver enhver mulighed for at rapportere et digitalt sikkerhedsproblem til organisationen. CVD-politikken skal definere trinene i den ansvarlige afsløringsproces og omfatte en kommunikationskanal for rapportering af sårbarheder. Bug bounty-programmer kan også bruges som en del af CVD-strategien.

Konformitetsvurdering

1. **Modul A:**
   Selvvurdering (for produkter, der hverken er vigtige eller kritiske).
2. **Modul B + Modul C:**
   Involverer en uafhængig vurderingsinstans.
3. **Modul H:**
   Involverer også en uafhængig vurderingsinstans.
4. **Certificering under en europæisk ordning i henhold til Cybersecurity Act.**
   Især EUCC-certificering på et niveau af sikkerhed, der er mindst "substantiel", fritager for tredjeparts konformitetsvurdering.

Produktets supportperiode og sikkerhedsopdateringer

Supportperioden for et produkt må ikke være mindre end 5 år, eller den forventede brugsperiode, hvis denne er mindre end 5 år. Sikkerhedsopdateringer skal være tilgængelige i mindst 10 år, selvom produktets supportperiode er kortere. Opdateringer skal distribueres automatisk og uden forsinkelse.

EU-overensstemmelseserklæring og CE-mærkning

Efter en konformitetsvurderingsprocedure skal fabrikanterne udarbejde en EU-overensstemmelseserklæring og anbringer CE-mærkningen.

EU-overensstemmelseserklæringen skal udarbejdes i overensstemmelse med modellen i Annex V i forordningen og skal opbevares til rådighed for markedsovervågningsmyndighederne i mindst 10 år efter, at produktet er bragt i omsætning.

Hvorfor handle nu?

Compliance handler ikke kun om at undgå bøder – som kan være op til 15 millioner euro – men også om at beskytte din virksomhed mod cybertrusler og sikre, at dine produkter lever op til markedets stigende sikkerhedskrav. Denne tilgang sikrer, at cybersikkerhed bliver en integreret del af din virksomheds praksis, så du står stærkt i fremtidens digitale landskab.

Praktiske værktøjer og løsninger

I dette afsnit angriber vi sikre systemer fra to vinkler:

1.Top-down model for konkret implementering af sikre systemer og

2. Basal cybersikkerhed, hvor vi fokuserer på det, som er nødvendigt lige nu og her – for SMV'er handler det om at implementere essentielle sikkerhedsfunktioner, der sikrer, at produkter kan opdateres og tilpasses fremtidige krav, selv med begrænsede ressourcer.

Hvordan du konkret implementerer datasikkerhed i udviklingsprocessen

Af Andreas Magnussen
Senior Consultant

"Top-down model": Sådan implementerer du sikre systemer

Dette afsnit giver retningslinjer for implementering af sikre systemer. I dag skal systemer også være robuste over for forsætligt misbrug i et muligt sikkerhedsangreb. Med andre ord skal systemet være robust over for datasikkerhedsangreb. Implementering af et sikkert system og sikring af fortsat sikkerhed kræver en proces og implementeringsaktiviteter. I denne artikel vil vi beskrive de vigtigste aktiviteter fra den indledende planlægning til fuld drift.

Plan for at opnå sikkerhed

Først skal sikkerhedsmålene defineres, herunder produktkrav, og lige så vigtigt, proceskrav. Planen skal også beskrive de beviser, der er nødvendige for at dokumentere resultaterne. Endvidere skal planen beskrive en strategi for at nå sikkerhedsmålene, f.eks. angivelse af planlagt teknologi.

- Organisation og interessenter og deres ansvarsområder skal defineres og justeres efter behov. At sikre datasikkerhed omfatter mange aktiviteter i løbet af produktets levetid.

- Lav en plan for implementering af datasikkerhed (fra indledende design, udvikling og implementering til produkterne er færdige). Det er en livscyklusproces, og din forretningsmodel skal understøtte dette.

- Definér sikkerhedsniveauet - f.eks. kundernes forventninger eller certificeringsniveauer. Sikkerhedsarbejde (og certificering) kan være dyrt, og det er vigtigt med en klar retning og strategi.

- Beskriv de processer, der er nødvendige for at nå sikkerhedsmålene.

- Beskriv aktiviteterne og hvad der er nødvendigt for at gennemføre aktiviteten.

Udfør en risikovurdering af systemet

Sikkerhedsmålet er at sikre, at systemet fungerer som forventet, og at sikkerheden opretholdes, f.eks. den klassiske fortrolighed, integritet og tilgængelighed, men det kan være mere detaljeret.

Risikovurderingsanalysen skal identificere **alle** trusler, mulige angrebsscenarier, afhjælpninger og udføre en evaluering.

- Hvilke trusler skal systemet være robust over for?
- Hvad er systemgrænserne og de eksterne grænseflader? Hvad er de anvendte datastrømme og protokoller? Alle protokollag skal identificeres.
- Identificér og analyser alle mulige kommunikationsveje.
- Hvordan kan en angriber komme ind i et sub-system og videre til næste system?

En metode til identifikation af sårbarheder og angrebsmetoder bør omfatte søgning i offentlige databaser over kendte sårbarheder (f.eks. CVE) efter anvendte protokoller og lignende. Angribere kan være meget kreative og søge efter implementerbare sårbarheder. **"Zero day"** (nye) sårbarheder, som ikke er offentligt kendte, er vanskelige at forudsige, men generelle scanninger og evalueringer kan give en indikation af nye angrebsmetoder, som systemet bør være robust overfor.

Fælles eller delte ressourcer indebærer en **sikkerhedsrisiko**, og **sårbarheder er mulige mål for angreb**. Delte ressourcer som et processorsystem kan potentielt bruges til at angribe nabomoduler. **Når du analyserer, skal du antage, at hvert modul er kompromitteret**, og analysere alle kommunikationsstier fra det pågældende modul.

Planlægning og dokumentation

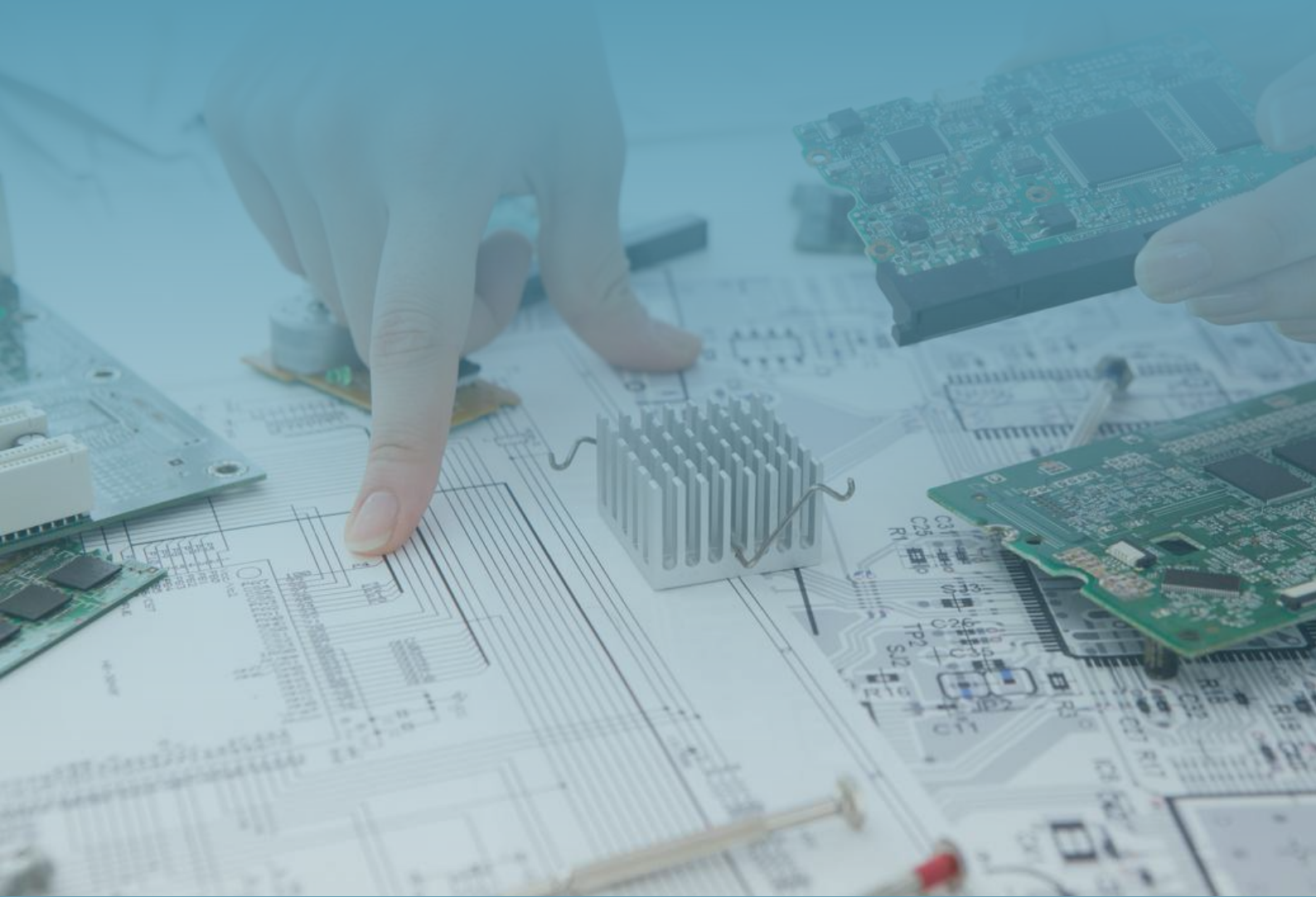
Dokumenter alle resultater. Sikkerhedsbeskyttelsen ændrer sig over tid, og det er vigtigt at vide, hvordan systemet er designet og testet.
Det er sandsynligt, at testen skal opdateres og udføres igen, og at koden skal opdateres. Det flydende emne bør behandles i planlægningsfasen.

- Sikkerhedstruslerne kan ændre sig over tid, og der kan blive opdaget nye sårbarheder, og risikovurderingen skal revurderes.

- Sikkerhed er dynamisk; angribere vil altid forsøge at angribe systemerne og finde nye måder at angribe på og bruge nye sårbarheder.

- Effekten af et angreb er normalt konstant over tid, mens sandsynligheden for et angreb kan stige, hvis der opdages nye angrebsmetoder eller sårbarheder. Virkning og sandsynlighed skal beskrives og dokumenteres.

- Hvordan kan systemet eller softwaren opdateres i tilfælde af sikkerhedshuller med stor effekt?



Implementering

Softwaren og systemet skal designes, så en enkelt fejl ikke kan forplante sig til andre funktioner ved et bevidst angreb. Implementér systemet med flere lag af uafhængig sikkerhedsbeskyttelse (sikkerhedsforanstaltninger). Og sørg for robusthed mellem moduler og ved eksterne grænseflader. Hvis et system f.eks. bliver tilsluttet, skal de tilsluttede systemer være robuste over for sikkerhedsangreb, så angrebet ikke påvirker flere systemer.

Kodningsstile bør være forsvar. Brug kodekontrolværktøjer til statisk kodeanalyse og helst værktøjer til måling af kodedækning.

De fleste systemer i dag bruger eksisterende tilgængelig software, ofte kaldet **COTS** (commercial-off-the-shelf), såsom OS, platformssoftware, biblioteker, værktøjer og applikationer. **Brug af eksisterende software kræver særlig opmærksomhed**, fordi software højst sandsynligt har flere sårbarheder.

- Omhyggelig udvælgelse og dokumentation af brugt COTS. Der er ofte flere tilgængelige distributioner, og sikkerhedsbevidsthed bør være et evalueringskriterium.

- Evaluer kendte sårbarheder og lav en plan for hærdning og løbende overvågning af sårbarheder.

- Evaluér konfigurationen. Forkert konfiguration kan resultere i usikre systemer.

Ved opstart af systemet bør man overveje at stole på bootloaderen og eventuelt **få bootloaderen til at udføre en integritetskontrol**. Hvis der ikke er fuld tillid til opstartskæden, kan det være meget vanskeligt at sikre sikkerhed og integritet i systemet.

Test af sikkerhed

Essensen af **sikkerhedstest er out of spec-test**. Kan systemet tvinges ind i en uventet adfærd, som kan føre til en ændret systemadfærd, og i sidste ende kan en angriber muligvis tage kontrol over systemet. Sikkerhedstest bør omfatte:

- Robusthedstjek af funktioner, der sikrer sikkerhed. Bemærk, at små svagheder ofte kan udvikle sig til regulære sikkerhedshuller. Al uventet adfærd bør analyseres, fordi det kan være en reel svaghed eller sårbarhed.

- Der bør udføres sikkerhedstest i alle lag (også internt). Test f.eks. hvert lag uafhængigt af hinanden.

- Penetrationstests af system, moduler og protokoller. Det kan være nødvendigt at implementere testfunktioner for at få adgang til interne protokoller under test. Der findes mange værktøjer.

Sikkerhedsovervågning og fortsat sikker drift

Opretholdelse af sikkerheden efter den første udrulning kræver metoder til at overvåge adfærden for at sikre, at systemet fungerer som forventet. Hvordan dette kan implementeres, afhænger af servicemodellen, tilslutningsmuligheder, sikkerhedskrav og regulære krav (f.eks. certificering).

Aktiviteterne kan grupperes i følgende kategorier:

- Interne systemfunktioner til overvågning af systemet:
  - Overvåg kode- og datakonsistens, f.eks. signaturkontrol.
  - Log hændelser i sikkerhedsloggen.

- Eksterne funktioner:
  - Ekstern overvågning af adfærd, f.eks. logning eller overvågning af ekstern trafik, eller logning af en væsentlig del af den eksterne trafik.
  - Sikkerhedslogs og behandling af sikkerhedshændelser.

- Sikkerhedsproces:
  - Scan efter sårbarheder i CVE-databaser eller sikkerhedspapirer, og vurder mulige sikkerhedsmæssige konsekvenser for systemet. Kan denne type sårbarhed f.eks. bruges til at angribe systemet?

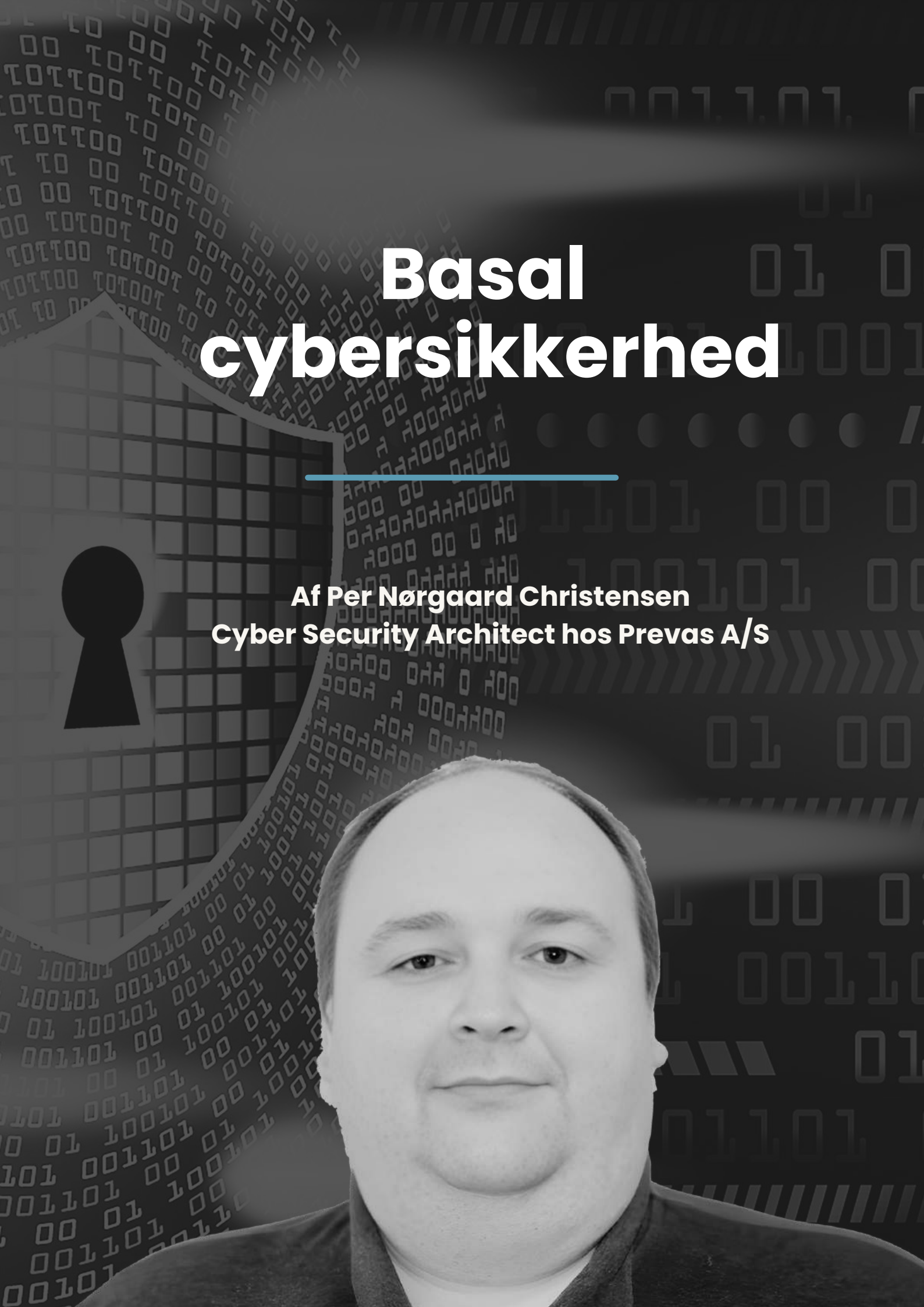
Generelle råd

Liste over ting, der skal overvejes:

- Udfør en teknologievaluering for alle funktioner, der implementerer sikkerhed. Hvor robust er implementeringen, og hvilken ekstern eller intern adfærd kan påvirke driften af funktionen?
- Brug datasikkerhed til en generel forbedring af kvalitet og dokumentation. F.eks. kravstyring, sporbarhed af krav og nedbrydning af krav.
- Der skal være en strategi for genopretning og restaurering fra anvendte backup systemer.
- Sikring af integritet før og efter et angreb i alle dele af systemet. Signering af software og softwarekomponenter kan være en løsning. Dataintegritet skal også overvejes.

Basal cybersikkerhed

Af Per Nørgaard Christensen
Cyber Security Architect hos Prevas A/S



Basal cybersikkerhed

Hvis man er en lille eller mellemstor virksomhed (SMV) er det ikke givet, at man har ressourcerne til at kan kaste sig ud i en risikobaseret tilgang til cybersikkerhed, da det ofte kræver en del tid og mange ressourcer, som ikke nødvendigvis hænger på træerne. Ofte vil det også være en prioritet mellem cybersikkerhed og nye smarte unikke selling points.

Derfor vil vi her i det efterfølgende introducere de basale cybersikkerheds features, som er nødvendige for at et produkt efterfølgende kan opdateres med nye features, når det er kommet på markedet eller ud til kunderne.

Vi kommer ind på følgende områder:

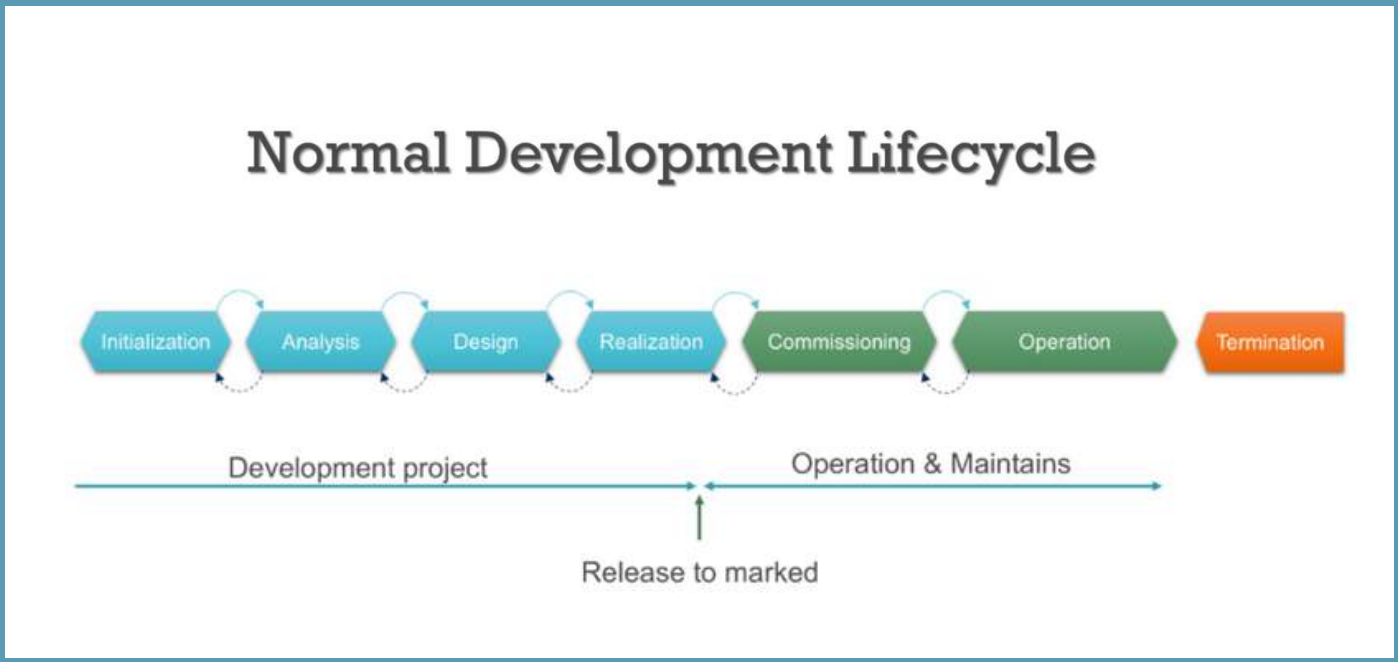
- Udviklingen:
  - Projektmodel med indbygget cybersikkerhed
  - Håndtering af nøgler til kodesignering
  - Bygge og teste pipelines (CI/CD)
  - Løbende overvågning og reaktion på CVE'er

- Produkt features:
  - Secure boot - Root of Trust (RoT) / Chain of Trust (CoT)
  - Secure storage
  - Secure update
  - Secure debug
  - Secure hardware

- Produktion

Projektmodel med indbygget cybersikkerhed

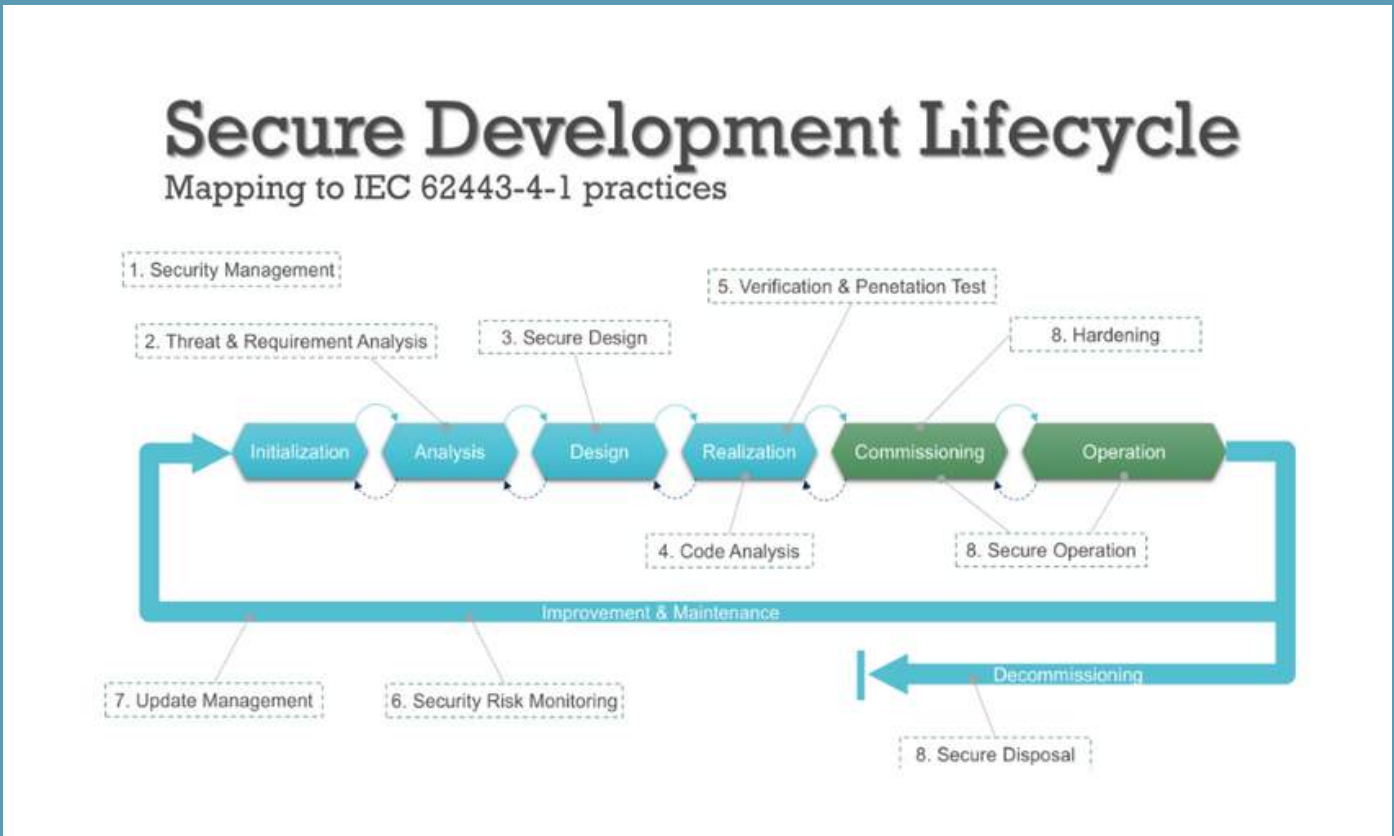
I et traditionelt state-gate produktudviklingsprojekt er processen lineær, forstået på den måde, at man starter med at få initialiseret og defineret projektet og derefter følger selve udviklingen/skabelsen/realisering af produktet inden det sættes i produktion/drift.
Når produktet så er frigivet til markedet, stopper udviklingsprojektet og overgår i en drift- og vedligeholdes fase, som bliver ved indtil produktet tages af markedet.



Cybertruslen i dag udfordrer denne måde at køre udviklingsprojekter på. Der vil løbende komme nye sårbarheder som hackerne finder og udnytter.
Derfor skal der løbende være fokus på at holde produktet opdateret og udbedre de sårbarheder, som måtte være.

Dette er bl.a. noget af det som den nye CRA har fokus på. Hvis ikke man sørger for at holde produktet opdateret, vil det resultere i, at produktet ikke længere vil være sikkert at bruge og kan dermed være indgangsvinklen for et cyberangreb hos kunderne.

Dette kan koste dyrt på troværdighed af produktet og virksomhedens omdømme, hvilket med stor sandsynlighed vil kunne **aflæses i et mindre eller større fald i salget.**



Et cybersikkerhedsprojekt skal opfattes som en dynamisk og løbende proces, over hele produktets samlede levetid. Dette indebærer:

- **Sikkerhed som grundsten:**

Cybersikkerhed integreres i alle faser – fra design og udvikling til drift og endelig terminering.

- **Løbende opdateringer:**

Regelmæssige softwarepatches og sikkerhedsforbedringer for at adressere nye trusler. En del af det løbende beredskab er, at man kan lave hotfix's som hurtigt kan lukke kritiske sikkerhedshuller i løbet af kort tid.

- **Livscyklusperspektiv**:

Løbende overvågning af sårbarheder, nye risikovurderinger og vedligeholdelse skal være med til at opretholde produktets cybersikkerhed gennem hele dets levetid.

Hovedaktiviteter for et cybersikkerhedsprojekt

1. **Security by Design:**
Cybersikkerhed planlægges og implementeres fra starten for at identificere og reducere sårbarheder.

2. **Opdateringer og patching:**
Nye sikkerhedspatches og softwareopdateringer skal leveres løbende gennem hele produktets levetid.

3. **Automatiseret bygge- og test-pipelines:**
Implementering af CI/CD er med til at sikre en hurtig og pålidelig release af softwaren. Automatiserede tests hjælper med at identificere potentielle fejl og sårbarheder tidligt i udviklingen.

4. **CVE-overvågning:**
Løbende overvågning af software for kendte sårbarheder (f.eks. gennem CVE-databaser) sikrer, at potentielle risici håndteres proaktivt.

5. **Sikker nøglehåndtering:**
Implementering af procedurer til beskyttelse af kodesigneringsnøgler og enhedsnøgler er afgørende for at opretholde produktets integritet.

6. **Sikker produktion:**
Etablering af sikre produktionsprocesser, herunder håndtering af unikke nøgler for hver enhed, er kritisk for at beskytte data og forhindre angreb.

7. **Vedligeholdelse af udviklingsmiljø:**
Udviklings- og byggemiljøer skal løbende opdateres og vedligeholdes for at undgå afhængighed af forældede teknologier.

Infrastruktur til kodesignering

En vigtig del af cybersikkerheden er, at man kan stole på, at den software man leverer, rent faktisk kommer fra én selv. Dette sikres ved at signere softwaren, så den kan verificeres, inden den eksekveres på target-enheden.

Signering af software kræver brug af særlige signeringsnøgler, ofte kaldet kodesigneringsnøgler. Disse nøgler udgør typisk et public/private key-par, hvor den offentlige nøgle (public key) ligger på det system, softwaren installeres på, og bruges til at verificere softwarets integritet og oprindelse. Den private nøgle anvendes i forbindelse med softwareudgivelser til selve signeringsprocessen. Den private nøgle er derfor ekstremt kritisk, da den er garant for softwarets autenticitet. Hvis denne nøgle kompromitteres, kan en tredjepart – eksempelvis en hacker – potentielt indsætte malware i softwaren og efterfølgende gensignere den. Dette kan gøre det umuligt at opdage, at softwaren er blevet manipuleret.

Kodesignering udgør grundlaget for tillid og sikkerhed i software, da det sikrer, at den udgivne software er autentisk og uændret. Men tab af eller kompromittering af disse nøgler kan få katastrofale konsekvenser – lige fra tab af virksomhedens omdømme til betydelige økonomiske skader. Det som mange glemmer, er at signeringsnøglerne er nøglerne til ens forretning – dette er ofte et overset aspekt blandt virksomhedens ledelse.

Derfor er det essentielt at etablere en robust infrastruktur til at beskytte og administrere disse nøgler.

Sådan sikrer du korrekt nøglehåndtering:

1. **Begræns adgang til nøgler:**
Kun autoriseret personale bør have adgang til kodesigneringsnøgler, og alle aktiviteter skal logges og overvåges for at sikre ansvarlighed. Ligeledes bør nøglerne kun være tilgængelige, når de skal anvendes.

2. **Fysisk sikkerhed:**
Opbevar nøglelagringsenheder i sikre beholdere eller lokationer, såsom låste skabe eller bokse, for at minimere risikoen for tyveri. Derudover bør der være lavet back-up af nøglerne, som fysisk placeres andet sted for at sikre mod brand eller anden ødelæggelse af lagringsenheden.

3. **Brug af stærke adgangskoder:**
Hvis de private nøgler opbevares som filer, anbefaler vi kraftigt at beskytte dem med stærke og unikke adgangskoder for at forhindre uautoriseret adgang. Det frarådes dog generelt at opbevare nøgler som filer. Brug i stedet en dedikeret HSM- eller smartkey-løsning – eller en sikker cloud-baseret HSM-signeringsløsning – for at opnå højere sikkerhed.

4. **HSM (Hardware Security Module):**
Implementér HSM-løsninger, der opfylder industristandarder (f.eks. FIPS 140-2), for at sikre, at nøglerne forbliver sikre og beskyttet mod både interne og eksterne trusler. En god idé er at anvende HSM'er som kan understøtte PKCS#11, da mange kodesigneringsværktøjer kan interface til denne standard.

5. **Separate certifikater til test og produktion:**
Brug forskellige certifikater til udvikling og produktion. Testcertifikater bør kun anvendes i udviklingsmiljøer og aldrig på produktsystemer.

En stærk nøgleadministration reducerer ikke kun risikoen for angreb, men opretholder også kundernes tillid til din virksomhed. Et kompromis på dette område kan føre til betydelige omkostninger – ikke kun økonomisk, men også omdømmemæssigt. Derfor bør nøglehåndtering være en integreret del af enhver organisations sikkerhedsstrategi.

Automatiseret bygge- og testmiljø

For løbende at kunne levere hurtige og pålidelige software-releases er et automatiseret bygge- og testmiljø afgørende. Uden et velfungerende og opdateret system risikerer man at bruge unødvendig lang tid og ressourcer på manuelle processer, som kan føre til fejl og forsinkelser – specielt når der er tale om en kritisk software-release, som skal ud hurtigst muligt for at lukke et kritisk sikkerhedshul.

Vigtige elementer i et automatiseret bygge- og testmiljø:

Secure bygge-pipelines: Implementér bygge-pipelines med build-servere for at sikre kontinuerlig integration og levering. Disse pipelines automatiserer trin som kompilering og signeringen af softwaren.

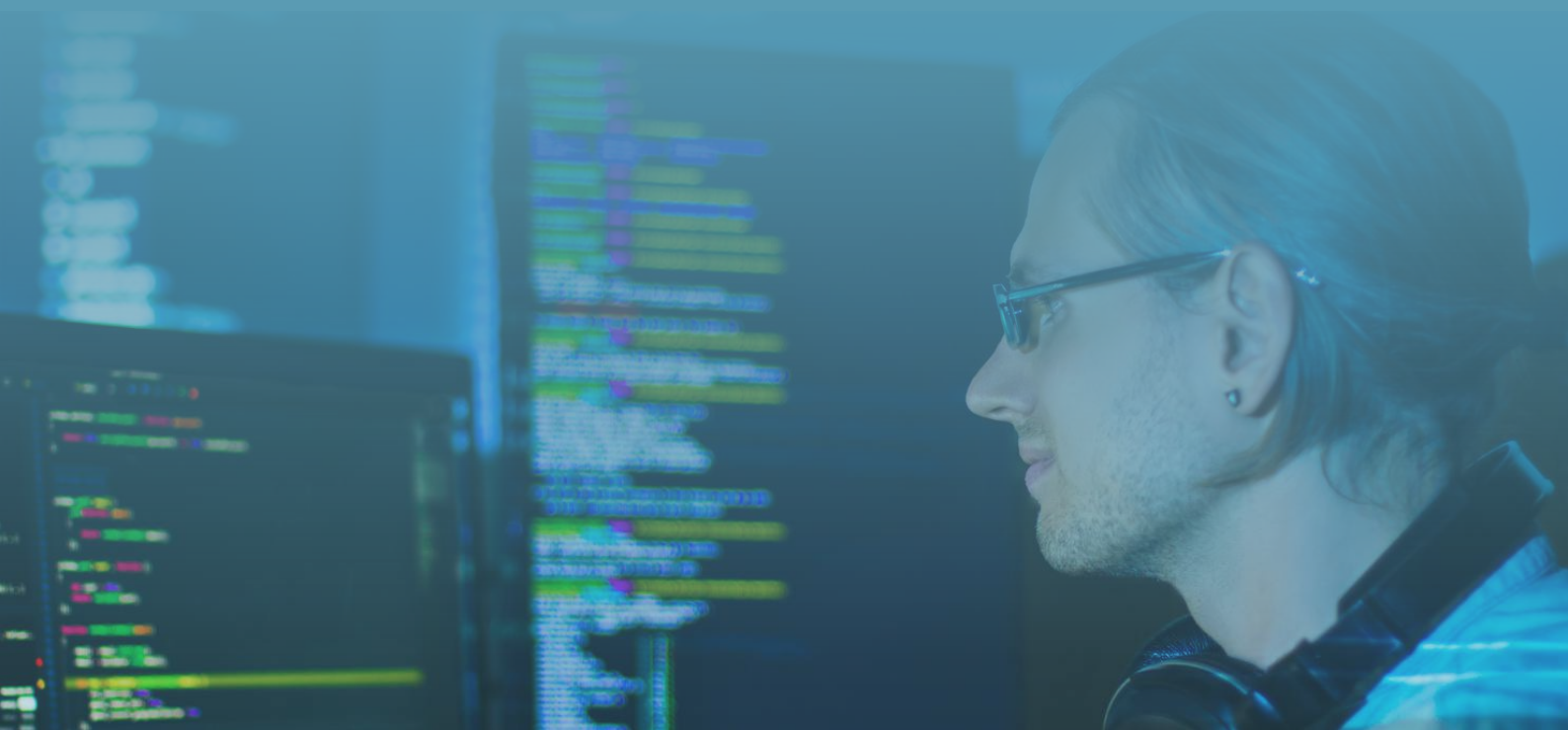
Secure automatiserede testmiljøer: Test-pipelines bør inkludere automatiserede testopstillinger (test racks) for at efterligne virkelige scenarier og identificere potentielle fejl tidligt i udviklingsprocessen.

- **Integration og performance-test:**

Integrationstests sikrer, at systemets forskellige moduler fungerer sammen, mens performance-tests måler systemets ydeevne under realistiske belastningsforhold.

- **Regressionstests:**

Regressionstests og miljøtests er nødvendige for at simulere virkelige anvendelsescases og vurdere systemets sikkerhed og stabilitet i varierende miljøer.



Anbefalinger til test-setup:

1. Brug enten open-source eller andre frameworks til testudførelse.
Det sparer udviklingstid og sikrer fokus på selve testcase udviklingen.
-> Opfind **ikke** dit eget testframework, da det kun er med til at stjæle tid og dermed øgede omkostninger.

2. Forvent, at udvikling af testcases tager lige så lang tid som kodning.
Dette er en god tommelfingerregel, der sikrer, at der allokeres tilstrækkelige ressourcer til at opbygge et robust testmiljø.

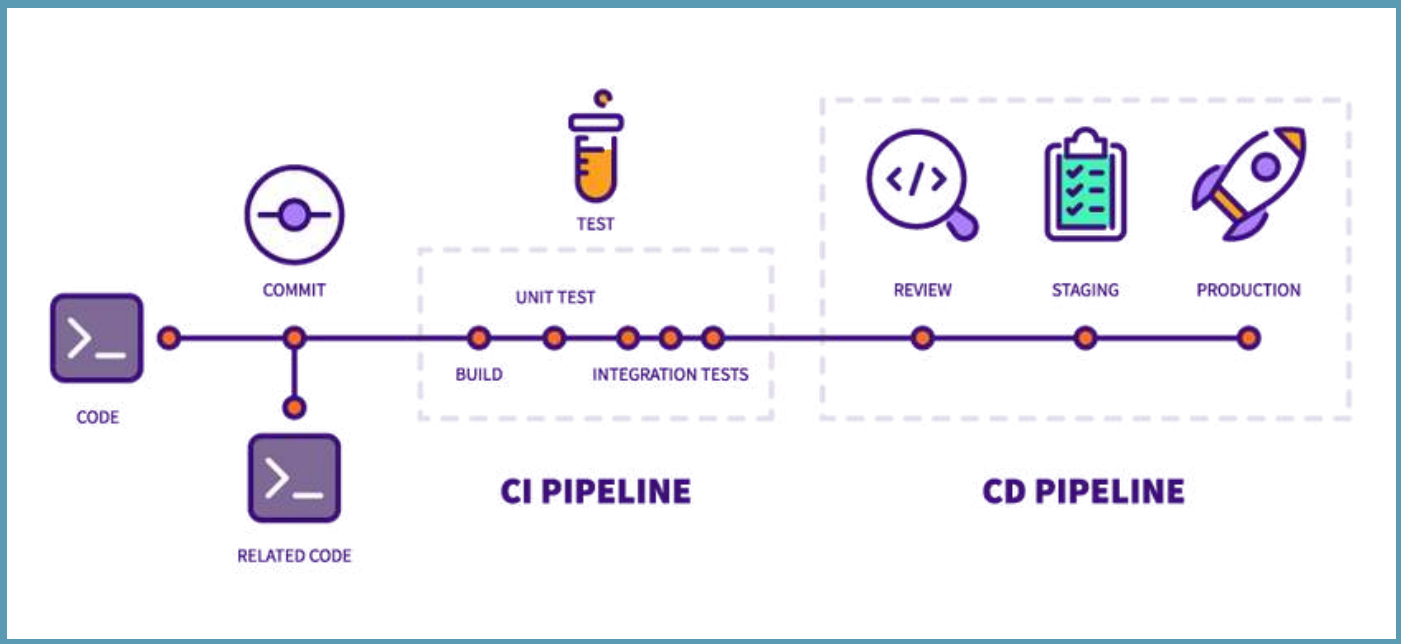
Fordele ved automatisering:

- **Reduceret time-to-market:** Automatiserede processer muliggør hurtigere levering af opdateringer og forbedringer.

- **Forbedret kvalitet:** Med grundige tests i alle faser af udviklingen reduceres risikoen for fejl i den endelige software.

- **Skalérbarhed:** Automatiserede systemer gør det lettere at håndtere komplekse systemer og større produktporteføljer.

Et automatiseret bygge- og testmiljø er derfor ikke blot en investering i effektivitet, men også i kvalitet og pålidelighed, som sikrer, at softwareudviklingen lever op til moderne krav om sikkerhed og ydeevne.



Overvågning af CVE'er (Common Vulnerabilities and Exposures)

Løbende overvågning af CVE'er er en kritisk opgave for at sikre, at software i drift forbliver beskyttet mod kendte sårbarheder. Denne proces sikrer, at potentielle trusler identificeres og håndteres hurtigt, før de kan udnyttes af angribere.

Vigtige elementer i CVE-overvågning:

1 Daglig overvågning:

- Hold øje med CVE-databaser som f.eks. NVD (National Vulnerability Database) fra NIST for at identificere nye sårbarheder, der kan påvirke din software.
- Brug værktøjer som Yocto til at holde din Software Bill of Materials (SBOM) opdateret. Dette kræver dog en ekstra indsats for at inkludere overvågning.
- Brug et overvågningsværktøj eller en CI/CD-pipeline til løbende at holde øje med ændringer i CVE-databasen som har indflydelse på de softwarepakker som indgår i SBOM'en. En god idé er at have et overvågningsværktøj, som har en slags "keep-alive"-mekanisme, som kan sikre at overvågningen fungerer korrekt. En overvågning som udad til ser ud til at virke, men indad ikke fungerer korrekt f.eks. pga. manglende adgang til en CVE-database – giver falsk tryghed.

2 Evaluering af CVE'er:

- Filtrér CVE'er baseret på CVSS (Common Vulnerability Scoring System)-score og vurdér dem i forhold til din softwares anvendelse og specifikke funktioner.
- Udvikl en klar procedure til håndtering af CVE'er, herunder hvordan de skal prioriteres og løses. For eksempel: Hvis en CVE allerede er rettet i en nyere version af softwaren, bør en opgradering være første valg.

3 Planlægning og tidsstyring:

- Håndtering af CVE'er er en omfattende proces, og bør ikke betragtes som en sekundær opgave. Det kræver dedikerede ressourcer og løbende opmærksomhed for at sikre effektiv håndtering.

Hvorfor CVE-overvågning er vigtig:
Ved at integrere CVE-overvågning i din organisations sikkerhedsprocesser kan du proaktivt beskytte din software og minimere risikoen for sikkerhedsbrud.

Det understøtter også compliance med **lovgivninger som EU's Cyber Resilience Act og styrker kundernes tillid til dine produkter**. Løbende overvågning af den software, man har i marken, i forhold til sårbarheder, er afgørende for at opretholde sikkerheden.

Løbende vedligeholdelse af software- og udviklingsmiljøer

Effektiv vedligeholdelse af software og tilhørende udviklingsmiljøer er afgørende for at sikre kontinuerlig drift, hurtige opdateringer og en fremtidssikret udviklingsproces. Det er vigtigt at undgå afhængighed af forældet udstyr eller software, der kan bremse udviklingshastigheden og øge risikoen for fejl.

Strategier for vedligeholdelse:

1 Opdateringsstrategi:

- Implementér en struktureret opdateringscyklus, der inkluderer både større og mindre softwareudgivelser.
- Følg etablerede release-cyklusser, som eksempelvis Yocto, og planlæg regelmæssige mindre opdateringer for at holde systemerne ajourført.

2 Forberedelse til hurtige rettelser:

- Hav procedurer på plads til at håndtere hotfixes og patches inden for 24 timer i tilfælde af kritiske sårbarheder eller fejl.

3 Vedligeholdelse af udviklingsmiljøet:

- Hold servere, PC'er og testudstyr opdaterede og funktionelle for at sikre, at udviklingsprocessen kan fortsætte uden afbrydelser.
- Sørg for, at testudstyr altid er klar til brug og i en stabil konfiguration.

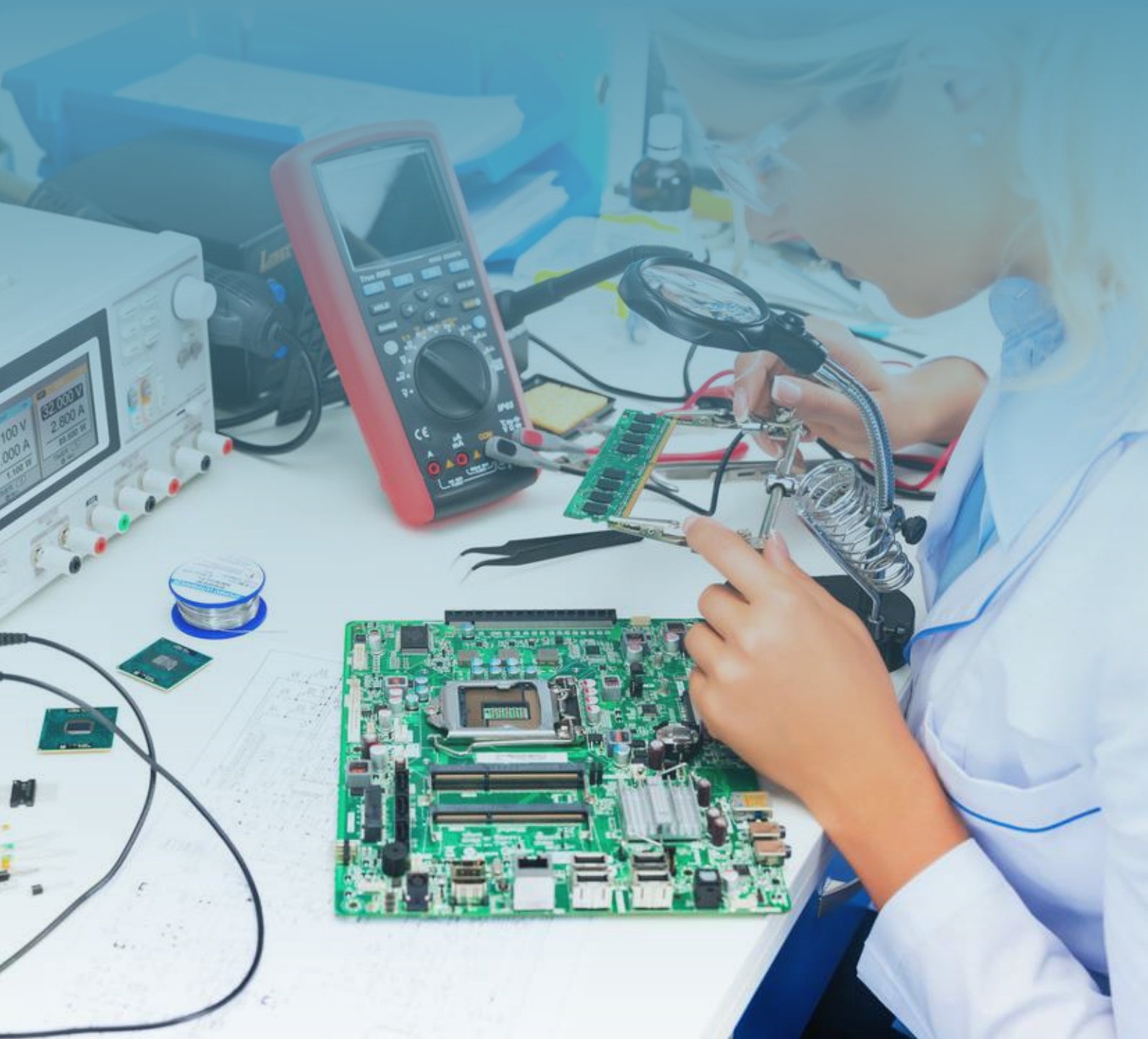
4 Opdatering af kildekoden:

- Undgå backporting ved at holde kildekoden opdateret til de nyeste stabile versioner.
- Små, regelmæssige opdateringer er mere omkostningseffektive og mindre risikable end at vente på større, omfattende opdateringer, som ofte kræver, at hele systemet bygges om fra bunden.

Hvorfor er vedligeholdelse vigtig?

Manglende vedligeholdelse kan føre til afhængighed af forældede systemer, hvor softwaren kun kan bygges på specifikke ældre computere med præcise konfigurationer.

Dette skaber flaskehalse og øger risikoen for fejl, især hvis udstyret svigter. Ved at prioritere vedligeholdelse sikres et robust og fleksibelt udviklingsmiljø, der kan understøtte fremtidige behov og udfordringer.



Sikker produktion: Implementering af Root of Trust (RoT)

Opbygning af en sikker produktionsproces er en kritisk del af moderne elektronikudvikling. Mange virksomheder undervurderer omfanget og kompleksiteten af at sikre produktionen, især når det kommer til håndtering af data og nøgler på en sikker måde.

En af de mest udfordrende opgaver er at generere og håndtere unikke nøgler for hver enkelt enhed. Dette kræver en robust proces, der ikke alene sikrer integriteten af nøglerne, men også beskytter dem mod kompromittering gennem hele enhedens livscyklus.

Nøgleelementer i en sikker produktionsproces:

1 Validering og sikkerhed:

- Verificér chip-leverandørens attesteringscertifikat for at sikre, at hardwaren kommer fra den rigtige leverandør og ikke er en kopivare med bagdøre.
- Brænding af offentlige nøgler i secure boot-sektionen for at skabe en sikker opstartsproces.

2 Unikke nøgler pr. enhed:

- Auto-genererede nøgler skal oprettes unikt for hver enhed og programmeres direkte ind i secure storage for at forhindre manipulation.

3 Identitetshåndtering:

- Læs og registrér enhedens UUID (universelt unikt ID) for at spore og administrere individuelle enheder effektivt.
- Generér og læs enhedens attesteringscertifikat (den offentlige del) for yderligere validering.

4 Integration med Device Management System:

- Opdater Device Management Systemet med de nye enheder, så hver enhed kan spores og administreres sikkert gennem dens livscyklus.

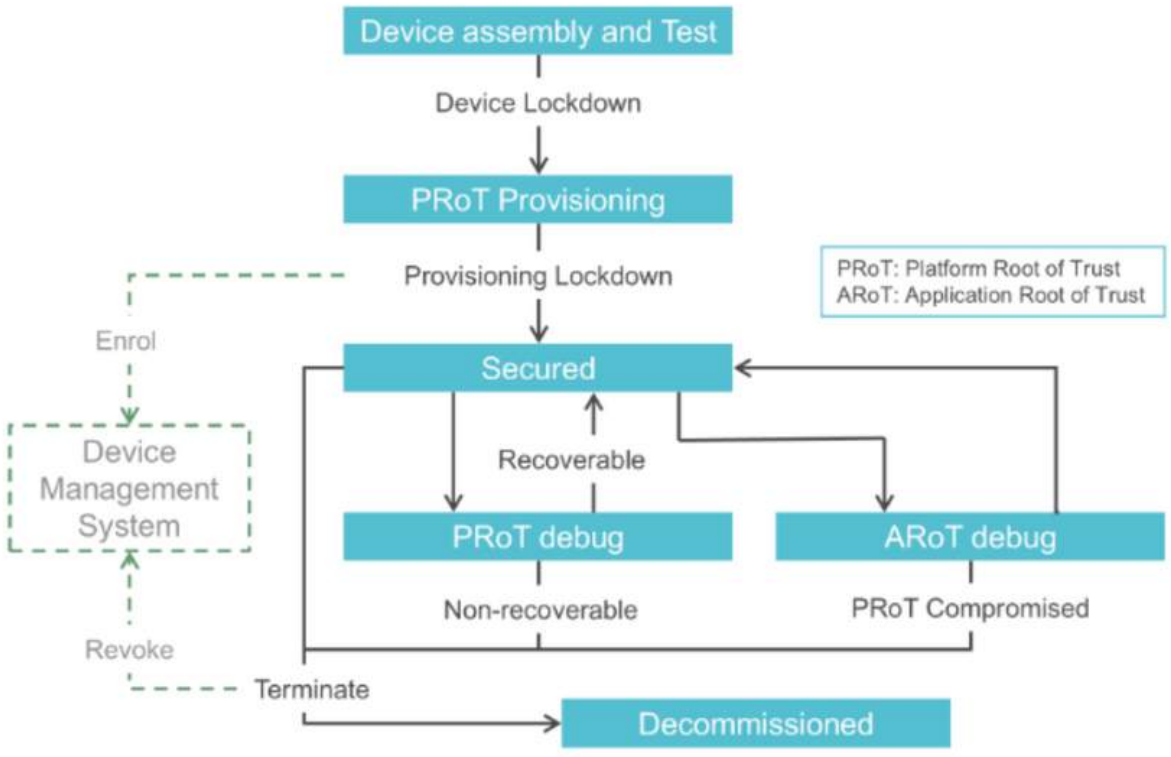
RoT-livscyklussen (Root of Trust):

- **Provisionering og lockdown:** Enheder skal låses sikkert under produktionen for at forhindre uautoriseret adgang eller ændringer.

- **Driftsfasen:** Enheder skal operere i en sikret tilstand med mulighed for gendannelse eller debugging i kontrollerede rammer.

- **Deaktivering:** Ved livscyklusens afslutning skal enhederne dekommissioneres, og deres data sikkert fjernes eller destrueres for at forhindre kompromittering.

En sikker produktionsproces, der inkorporerer Root of Trust-principper, er afgørende for at opretholde tillid og integritet i hele produktets levetid. Det kræver nøje planlægning, avancerede værktøjer og en forståelse af sikkerhed på tværs af både hardware og software.



Generic Platform Root of Trust (PRoT) security lifecycle

Softwareopdateringer og fleet management: Effektiv styring i feltet

For mange virksomheder er evnen til at distribuere softwareopdateringer direkte til produkter i brug – eller at lade produkterne selv sørge for at forblive opdaterede – en helt ny disciplin. Mange af vores kunder har ikke tidligere arbejdet med softwareopdateringer i marken, hvilket gør denne proces både udfordrende og afgørende.

Nøglekomponenter i en effektiv opdateringsstrategi:

1 Centraliseret styring:

- En løsning, der gør det muligt at udsende opdateringer til alle produkter på tværs af deres livscyklus. Dette inkluderer alt fra kritiske sikkerhedspatches til forbedringer af ydeevne og funktionalitet.

2 Automatisering:

- At lade enheder selv opdage og installere nødvendige opdateringer minimerer behovet for manuel indgriben og reducerer risikoen for fejl. Automatiserede processer sikrer, at ingen enheder bliver overset.

3 Feltopdateringer:

- Evnen til at opdatere software på enheder, der allerede er i brug, uden at påvirke deres stabilitet eller funktionalitet, er en nødvendighed. Det kræver fail-safe mekanismer, der kan håndtere fejl under opdateringsprocessen.

4 Sikkerhed som kerne:

- En sikker opdateringsproces, der sikrer, at kun autoriseret software installeres. Dette inkluderer brugen af digitale signaturer og sikre forbindelser under overførslen.

5 Livscyklusvedligeholdelse:

- Udvikling og vedligeholdelse af en opdateringsinfrastruktur, der kan håndtere produkternes krav, selv efter de er sendt på markedet.

For virksomheder, der endnu ikke har erfaring med fleet management og feltopdateringer, kræver det en betydelig omstilling. Men med de rigtige værktøjer og processer kan det forvandle deres evne til at reagere hurtigt på nye sikkerhedstrusler og ændrede markedskrav – og samtidigt sikre en høj standard for produktkvalitet og kundetilfredshed.

Basic Security Implementation

Grundlæggende Sikkerhedsimplementering

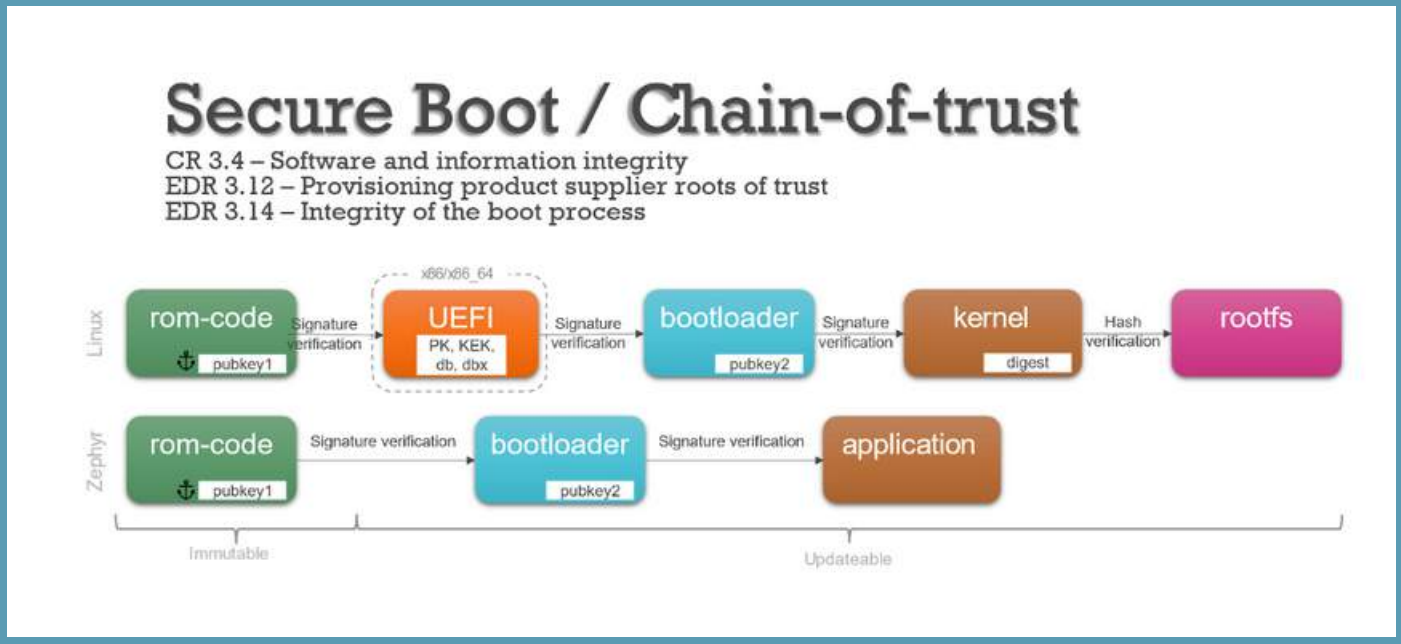
Basal sikkerhed i produktdesign er afgørende for at sikre systemernes integritet, fortrolighed og tilgængelighed. Ved at fokusere på essentielle sikkerhedsaspekter i hardware og software kan man reducere risici for sikkerhedsbrud og opretholde pålidelig drift i hele produktets livscyklus.

1 Roots of Trust

Roots of Trust (RoT) udgør fundamentet for sikkerheden i moderne enheder. Disse pålidelige hardware-, firmware- og softwarekomponenter sikrer kritiske sikkerhedsfunktioner. RoT danner grundlaget for tillid ved at sikre, at kun autoriseret software kan udføres på enheden. RoT kræver hardwareforankring, som for eksempel sikker opstart og brug af sikre nøgler. Dette skaber et sikkert fundament for hele enhedens livscyklus og muliggør en ubrudt kæde af tillid (Chain-of-Trust).

2 Secure Boot

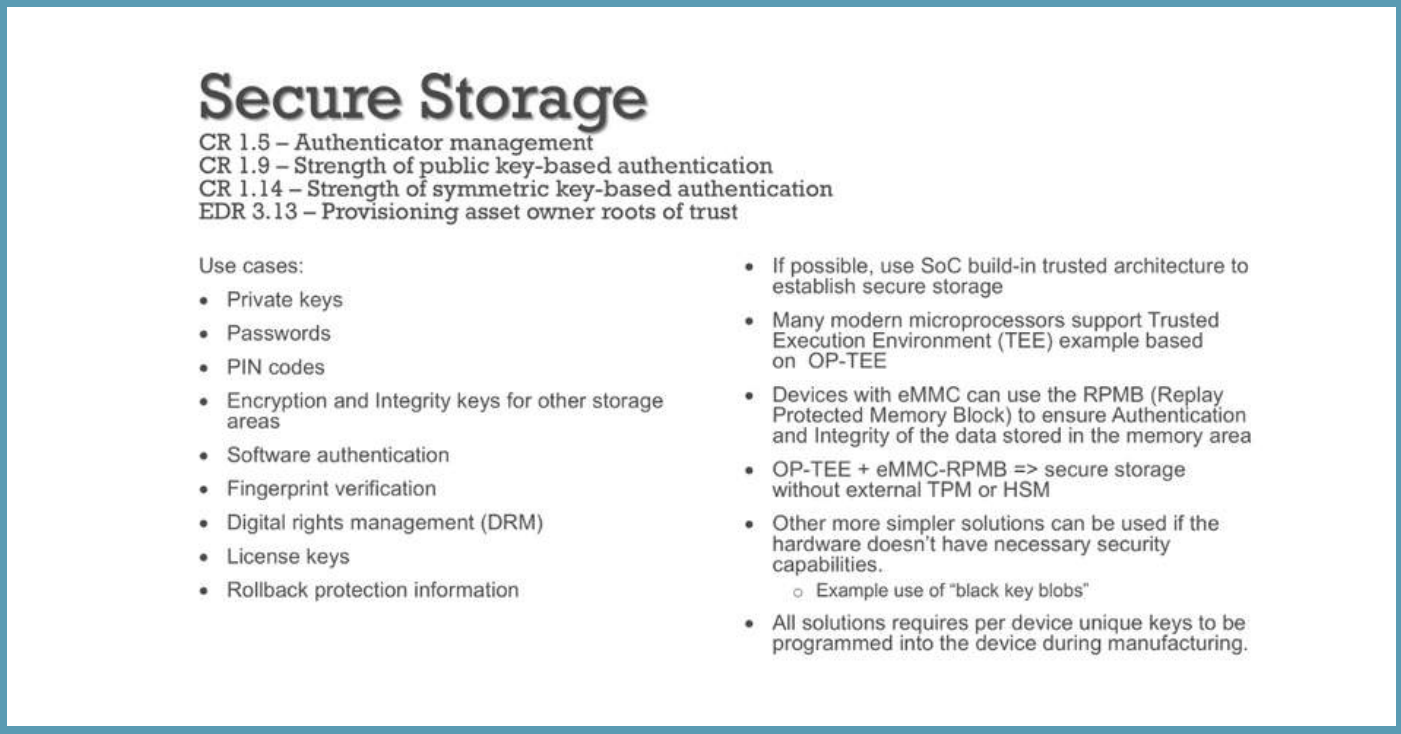
Secure Boot sikrer, at kun autoriseret software kan afvikles på enheden. Ved opstart verificeres hver komponent i kæden – fra rom-kode til applikation – ved hjælp af digitale signaturer. Den immutable del, såsom public-keys der skal bruges til at verificere bootloaderen, programmeres i efuses under produktionen, hvilket sikrer en dyb forankring af sikkerheden i hardwaren. Dette skaber en ubrudt kæde af tillid, der garanterer systemets integritet fra opstart til drift.



3 Secure Storage – sikker lagring af kritiske data

Sikker lagring af følsomme data som private nøgler, adgangskoder, certifikater og licensnøgler er afgørende for beskyttelsen af både system og bruger. Moderne mikroprocessorer indeholder i dag indbygget hardwarebaseret sikkerhed og små sikre processeringsenheder, som muliggør brugen af teknologier som Trusted Execution Environment (TEE) i kombination med eMMC Replay Protected Memory Block (RPMB). Denne løsning skaber en sikker lagringsmetode, der ofte er mere effektiv end brugen af eksterne TPM-moduler.

Ved nøje at vælge en eMMC med tilstrækkelig RPMB-kapacitet, kan man sikre, at alle nødvendige nøgler til produktets funktion lagres sikkert internt. Det adskiller sig fra TPM-baserede designs, hvor den begrænsede hukommelse ofte kræver, at krypterede TPM-nøgler gemmes i filsystemet som såkaldte "black key blobs".



Secure Storage

CR 1.5 – Authenticator management
CR 1.9 – Strength of public key-based authentication
CR 1.14 – Strength of symmetric key-based authentication
EDR 3.13 – Provisioning asset owner roots of trust

Use cases:

- Private keys
- Passwords
- PIN codes
- Encryption and Integrity keys for other storage areas
- Software authentication
- Fingerprint verification
- Digital rights management (DRM)
- License keys
- Rollback protection information

- If possible, use SoC build-in trusted architecture to establish secure storage
- Many modern microprocessors support Trusted Execution Environment (TEE) example based on OP-TEE
- Devices with eMMC can use the RPMB (Replay Protected Memory Block) to ensure Authentication and Integrity of the data stored in the memory area
- OP-TEE + eMMC-RPMB => secure storage without external TPM or HSM
- Other more simpler solutions can be used if the hardware doesn't have necessary security capabilities.
  - Example use of "black key blobs"
- All solutions requires per device unique keys to be programmed into the device during manufacturing.

4

Secure Update

Softwareopdateringer er essentielle for at håndtere sikkerhedsrisici og forbedre funktionaliteten. Kun autoriserede opdateringer skal tillades, og systemet skal være failsafe for at undgå nedbrud. Automatiserede flådeopdateringer giver mulighed for at opretholde sikkerheden i hele produktets livscyklus, hvilket er afgørende for moderne IoT- og netværksforbundne enheder.

5

Secure Debug – sikker fejlsøgning efter produktlancering

Fejlsøgning på et produkt, der allerede er i brug eller kræver service, kan være en stor udfordring, når enheden er sat i secure mode. Derfor bør man overveje kun at anvende mikroprocessorer, der understøtter secure JTAG/SWD-debugging.

Under produktionen kan der brændes en unik nøgle ind i enhedens eFuses, som – hvis funktionen er aktiveret – senere kan bruges til at åbne op for secure JTAG/SWD-adgang.

Det anbefales, at disse nøgler genereres automatisk som tilfældige og unikke pr. enhed. De bør behandles som fortrolige oplysninger og opbevares sikkert i en krypteret database, så autoriseret personale ved behov kan få adgang til dem i forbindelse med service og reparation.

6

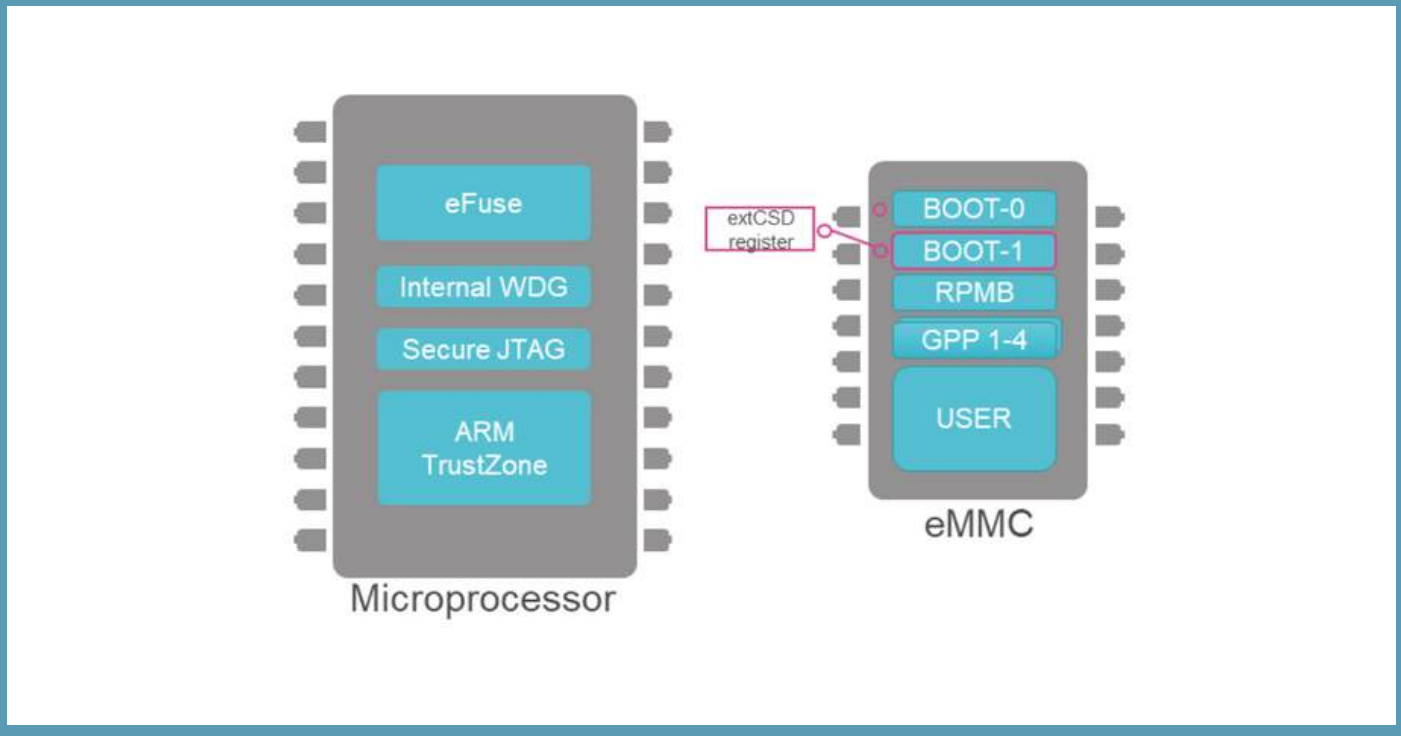
Fejlretning under produktudvikling og service skal ske sikkert

JTAG/SWD-debugging bør sikres med nøglebaseret adgang og deaktiveres, når det ikke er nødvendigt. Dette reducerer risikoen for uautoriseret adgang og sikrer, at fejlrettelse ikke bliver en svaghed i produktets sikkerhed.

7 Secure Hardware

Hardwaredesign skal minimere angrebsflader ved at deaktivere unødvendige interfaces. Moderne hardwaredesigns anvender eMMC-baseret lagring frem for gamle teknikker, såsom brug af spi-nor til bootload, eeprom til parameter og raw-nandflash kernel og root-filesystem. eMMC'en har den fordel, at den har indbygget RPMB hardware partition, som kan bruges til secure storage og boot partition, som kan være med til at lave sikre dual-copy systemer. Derudover kan der også konfigureres nogle generelle partitioner, der kan bruges til kalibreringsdata og andre produktspecifikke parametre.

Minimering af angrebsfladerne bør også føre til brug af interne features i mikroprocessoren såsom watchdog-timere fremfor at lave eksterne kredsløb. Dette er bl.a. med til at øge robustheden. Ved at designe hardware med sikkerhed som udgangspunkt, kan produkter modstå kompromittering af enkelte komponenter - uden at svække hele systemet.



Ved at integrere disse sikkerhedskomponenter i design- og produktionsprocessen kan virksomheder sikre deres produkter mod moderne cybertrusler. Det er ikke kun et krav i moderne lovgivning, men også en investering i robusthed og pålidelighed.

FAQ – De mest stillede spørgsmål

Når virksomheder forbereder sig på at implementere cybersikkerhed i overensstemmelse med **Cyber Resilience Act (CRA) og Radio Equipment Directive – Delegated Act (REDDA),** dukker en række tilbagevendende spørgsmål op. Her er nogle af de vigtigste:

1 *Hvordan forankrer vi cyber sikkerhed i vores organisation, når eksterne konsulenter er færdige?*

Mange virksomheder bekymrer sig om, hvordan de sikrer, at cybersikkerhed bliver en del af organisationen på lang sigt. Det handler om:

- At sikre videns overførsel fra konsulenter til interne medarbejdere.
- At etablere klare processer og ansvarsområder, så arbejdet kan fortsætte uafhængigt.
- At træne nøglepersoner, der kan drive indsatsen fremadrettet.
- Mentorordning

2 *Hvor meget kræver det af vores organisations involvering?*

Implementering af cybersikkerhed kræver samarbejde på tværs af organisationen. Typisk kræves:

- Ledelsesinvolvering til at fastlægge strategi og prioriteringer.
- Deltagelse fra produktudvikling, IT og kvalitet for at udføre analyser og implementere sikkerhedsløsninger.
- Løbende opfølgning og træning, så cybersikkerhed bliver en del af virksomhedens kultur.

3 *Hvad kræver det økonomisk for virksomheden?*

Omkostninger afhænger af virksomhedens størrelse og modenhed, men typisk inkluderer de:

- Engangsudgifter: Konsulenthonorarer, GAP-analyser og opdatering af systemer.
- Løbende udgifter: Vedligeholdelse, sikkerhedsopdateringer og træning af medarbejdere.
- Langsigtede investeringer: Justering af arbejdsgange og værktøjer for at integrere security by design.

4 *Hvordan kan vi integrere de nye krav i vores eksisterende udviklingsprocesser?*

Det kræver en struktureret tilgang:

- Gennemfør en GAP-analyse for at identificere, hvor dine nuværende processer skal tilpasses.
- Tænk sikkerhed ind i hele produktets livscyklus (security by design).
- Etabler vedligeholdelsesplaner for løbende opdateringer og håndtering af sårbarheder.

5 *Hvad får virksomheden ud af at forbedre cybersikkerhed?*

Hvis cyber sikkerhed implementeres smart så kan det give et kvalitetsløft. Slut kunder vil ofte være afhændige af produktets funktioner, så det skal overvejes hvordan cyber sikkerhed har værdi for kunder og hvordan en forretningsmodel kan udbygges til cyber.:

6 *Kan vi ikke nøjes med at ændre lidt hist og her? Vi behøver vel ikke at implementere secure boot eller opdatere resten af softwaren? Det er vel nok bare at lave en lille ændring?*

Mange gange oplever vi, at man forsøger at springe over, hvor gærdet er lavest. Et lille fix eller en patch her og der løser dog ikke nødvendigvis de sikkerhedshuller, der måtte være. Tværtimod giver det ofte en falsk tryghed hos slutbrugerne.

Ofte er det ældre platforme og softwareapplikationer, der ikke har været opdateret i lang tid – hvis de overhovedet har været opdateret. Problemet med små fixes og patches er, at det blot er symptombehandling, som ikke adresserer de underliggende problemer. Disse dækker ofte over sårbarheder, der har eksisteret længe, fordi man ikke har fulgt med og opdateret softwaren løbende.

IOT-miljøer er de basale sikkerhedsfunktioner ofte ikke blevet aktiveret fra starten af produktets levetid. Samtidig er det afgørende at sikre, at den software, der kører på produktet, stammer fra en selv eller en pålidelig underleverandør. At kunne stole på softwaren er essentielt for at kunne implementere andre sikkerhedsmekanismer såsom brugergodkendelse og verificering af software, der installeres.

Konklusion

Samlet set er konklusionen, at implementering af cybersikkerhed i dag er en fundamental nødvendighed for alle virksomheder, der udvikler produkter med digitale elementer, ikke mindst på grund af de nye lovkrav fra EU i form af **Cyber Resilience Act (CRA) og Radio Equipment Directive – Delegated Act (REDDA).**

Det er tydeligt, at cybersikkerhed ikke længere er et valg – det er en forudsætning for at forblive konkurrencedygtig og compliant på det europæiske marked. Men én udfordring skiller sig særligt ud og kalder til **"sense of urgency": Knapheden på ressourcer.** Implementering af cybersikkerhed kræver specialiseret viden, tid og dedikerede ressourcer. Vi ser allerede nu, at kapaciteten i markedet er presset – og jo tættere vi kommer på de afgørende deadlines i 2026 og 2027, desto sværere bliver det at finde den nødvendige ekspertise og support.

Derfor er det afgørende at handle nu:

Forstå reglerne og deadlines: CRA trådte i kraft i december 2024, og krav om hændelsesrapportering følger allerede i 2026.

Få styr på processerne: Implementér **"security by design"**, og skab procedurer for opdateringer og håndtering af sårbarheder.

Involver ledelsen: Cybersikkerhed er ikke kun et spørgsmål for R&D – det kræver en helhedsindsats i hele organisationen, herunder kvalitetssikring og ledelsesopbakning.

Planlæg for fremtiden: Sæt realistiske mål og udarbejd en compliance roadmap for at sikre løbende udvikling og vedligeholdelse af sikkerhedsprocesser.

Vær på forkant og vind tid: Dem, der starter tidligt, vil få en konkurrencefordel ved at kunne tilbyde sikre og dokumenteret compliant produkter, når kravene skærpes.

Ved at tage proaktive skridt nu, styrker din virksomhed ikke blot sin markedsposition, men minimerer også risikoen for dyre fejl, bøder og tabt omdømme.

Andreas Magnussen fremhæver, at implementering af datasikkerhed kræver en systematisk "top-down" tilgang. Dette indebærer en grundig planlægning med klare sikkerhedsmål, en detaljeret risikovurdering, der identificerer potentielle trusler, og en veldokumenteret implementeringsproces med robuste kodningsprincipper og valg af pålidelige komponenter. Løbende overvågning og dokumentation er essentielle for at sikre systemets sikkerhed over tid og beskytte mod både aktuelle og fremtidige trusler.

Per Nørgaard Christensen fremhæver dernæst, at en basal, men robust cybersikkerhedsstrategi er afgørende for SMV'er.
Dette involverer at integrere sikkerhed i alle faser af produktets livscyklus – fra design og udvikling til produktion og vedligeholdelse. Kernen er principper som "Security by Design", løbende overvågning af CVE'er, og sikker håndtering af nøgler.

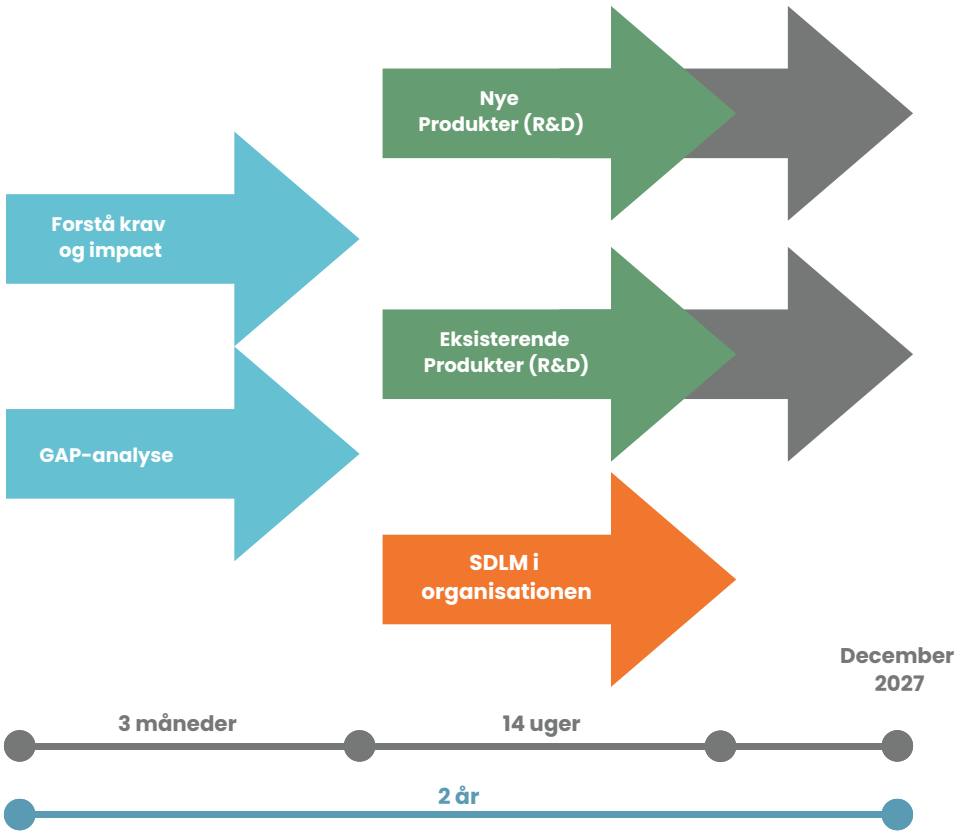
Sikre opdateringsprocesser er afgørende for at reagere hurtigt på trusler og bevare produktets integritet. Denne tilgang opfylder lovmæssige krav og styrker produktkvaliteten og kundetilliden.

Endeligt kan vi konkludere, at cybersikkerhed ikke længere er et valg, men en nødvendighed for at være konkurrencedygtig og overholde lovgivningen (CRA og REDDA). Ressourcemangel er dog en udfordring.

Derfor er proaktive tiltag afgørende: forstå reglerne, implementer robuste sikkerhedsprocesser, involver ledelsen, udarbejd en langsigtet plan, og søg hjælp, når det er nødvendigt. Tidlig handling giver en konkurrencemæssig fordel og reducerer risikoen for bøder og omdømmeskader.

E-bogen understreger yderligere, at en velstruktureret cybersikkerhedsstrategi ikke kun er et compliance-krav, men en strategisk investering i produktkvalitet, kundetillid og langsigtet konkurrenceevne. Ved at integrere sikkerhed i alle faser ("Security by Design"), implementere robuste processer og opbygge en kultur for løbende overvågning og forbedringer, kan virksomheder navigere effektivt i et komplekst trusselslandskab og levere sikre og pålidelige produkter. Proaktiv handling er afgørende for at opnå en stærk markedsposition og minimere risikoen for omdømmeskader og økonomiske tab.

Compliance Roadmap



Illustrationen viser et overblik over tidsforløbet for implementeringen af cybersikkerhed i henhold til Cyber Resilience Act (CRA).
Processen starter med at forstå krav og impact, efterfulgt af en GAP-analyse over en periode på 3 måneder.

Herefter bevæger processen sig videre til implementering i to hovedspor:

1. **Nye Produkter (R&D):** Her påbegyndes implementeringen af cybersikkerhed med en forventet varighed på 1-24 måneder, afhængigt af produktets kompleksitet og udviklingscyklus.
2. **Eksisterende Produkter (R&D):** Cybersikkerhed integreres løbende i eksisterende produkter for at sikre overholdelse af de nye krav.

Parallelt med disse aktiviteter implementeres **Secure Development Lifecycle Management (SDLM)** i organisationen, hvilket tager cirka 14 uger.
Samlet set strækker tidsrammen sig over **cirka 2 år**, hvor fuld integration af cybersikkerhed forventes opnået inden **december 2027, hvilket markerer afslutningen af overgangsperioden for CRA.**

Har du brug for hjælp til at komme i mål?

Flere af vores samarbejdspartnere, blandt andet Prevas, står klar til at hjælpe med alt fra GAP-analyser og risikovurderinger til implementering af praktiske sikkerhedsløsninger.

Book en afklarende samtale, og lad os sammen finde den rette vej for din virksomhed – og sikre, at I vinder tid og styrker jeres position på markedet.

Book her

engineer minds
we bring qualified people

+45 29 605 405 per@engineerminds.dk