Ramt af RED DA?

CYBERSIKKERHED OG COMPLIANCE

24/2-2026

Michael Stausholm, Principal Security Architect

Lidt om mig

- Uddannet datalog (kryptologi) i 2011.
- Har arbejdet med cybersikkerhed siden.
- Stort fokus på standarder og compliance de seneste år.
  - Sidder med i CEN/CLC JTC13 WG9

- Jeg ved en del om compliance, men jeg er ikke ekspert eller jurist (!)

Vi bringer den nyeste it-forskning og teknologi i spil i dansk erhvervsliv

- I kan bruge os som uvildigt konsulenthus eller underleverandør.
- I kan indgå i et af vores forsknings- og udviklingsprojekter.
- I kan deltage i vores netværk, workshops og arrangementer.

EU og Cybersikkerhed

- Cybersikkerhed har i høj grad været frivilligt
  - Kunderne har selv haft et ansvar for eksplicit at efterspørge sikkerhed
- EU har fået opmærksomhed på cybersikkerhed og lavet en del lovgivning
  - NIS 2, AI Act, DORA, DMA, DSA, CSA, osv.

- Også produkt lovgivning:
  - Radio Equipment Directive Delegated Act – RED DA
  - Cyber Resilience Act – CRA
  - Maskinforordning, Produktansvar, GPSR

RED DA

- Velkendt lovgivning der skal beskytte radionettet
  - Frekvenser, sendestyrke, EMC osv.

- Men også 3 ”delegerede akter” vedr. cybersikkerhed:

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(f) radio equipment supports certain features ensuring protection from fraud;

- De delegerede akter fik effekt i August 2025

RED DA – Hvad betyder det i praksis?

- Alle radioprodukter der sælges efter **1/8-2025** skal overholde *art. 3(3) (d), (e) og (f)*
- ”Radioudstyr” er alt som kan sende eller modtage radiobølger mhp. kommunikation, f.eks:
  - Mobiltelefoner, køleskabe med en wifi forbindelse, GPS modtager, osv.

- Rigtigt meget IoT falder i kategorien:
  - WiFi, Bluetooth, NFC, LoRa, Zigbee, 3G, 5G, osv.

- Kravene der skal overholdes afhænger af produktet:
  - *3 (3)(d):* Internet forbundet radioudstyr
  - *3 (3)(e):* Radioudstyr der behandler personfølsomt data
  - *3 (3)(f):* Radioudstyr der anvendes i forbindelse med finansielle transaktioner

Cyber Resilience Act

- Ny lovgivning der er bredere end RED DA
- Omfatter alle **produkter med digitale elementer**, incl. Software

- Fuld effekt 11 December 2027
  - Samtidigt tilbagetrækkes RED DA

- En del får dog effekt fra 11 September 2026 – ”Reporting obligations”
  - Hvis ens produkt er udsat for et aktivt hacker angreb, skal det indrapporteres til ENISA og CFCS

CRA

- Alle omfattede produkter skal overholde de samme krav !

- Der findes dog 4 produkt klasser som giver forskellige muligheder ifbm. compliance

Basic products	Important products Class I	Important products Class II	Critical products
• Anything else	• … • Microcontrollers with security-related functionalities • Smart home general purpose virtual assistants • Smart home products with security functionalities, including smart door locks, … • …	• Hypervisors and container runtime system • Firewalls, intrusion detection and prevention systems • Tamper-resistant microprocessors • Tamper-resistant microcontrollers	• Hardware Devices with Security Boxes • Smart meter gateways within smart metering systems… • Smartcards or similar devices, including secure elements

CE - mærkning

- CE er en selvdeklarering på at man overholde EU produktlovgivning
- Man er selv ansvarlig for at finde ud af hvilke love man er underlagt
- Forskellige love kan give forskellige muligheder for compliance, f.eks:
  - Selvevaluering (Modul A)
  - Selvevaluering med harmoniseret standard (Modul A)
  - Bemyndiget Organ / Notified Body (Modul B+C)
  - Cybersikkerhedscertficeringsordning (ifbm. CRA)

- BlueGuide: https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

Modul A

- Man vælger en egnet metode og dokumenterer man har anvendt den.
- Man skal kunne overbevise myndighederne om at den valgte metode er egnet

- I nogle tilfælde findes/kræves en ”citeret” harmoniseret standard.
  - EN 18031-1, EN 18031-2 og EN 18031-3 er citeret til RED DA art. 3 (3), hhv (d), (e) og (f)
- Anvender man en citeret standard, får man formodningsret og skal ikke kunne overbevise myndighederne om egnethed.

Standarder er ALTID frivillige at bruge, men de er ofte det ”lette” alternativ

Kvalitetssikring

- Tredjeparts vurdering er ikke et krav under Modul A
  - En uvildig gennemgang kan sikre kvaliteten
- Modul A er selvevaluering, så der er ikke formelle krav til hvordan kvalitetssikring foregår
  - Eksterne konsulenter kan hjælpe med udforming af dokumentation
  - Interne og eksterne kan validere den tekniske dokumentation

Notified body (Modul B+C)

- Myndighederne kan udpege ”bemyndigede organer” som kan udføre en typeafprøvning af produktet
- Det bemyndigede organ har kompetence til selv at vælge en egnet metode til afprøvningen
  - Et bemyndiget organ har i princippet ikke behov for en standard
  - Skal man til et bemyndiget organ, kan en DANAK akkrediteret rapport i nogle tilfælde indgå i vurderingen
- Certificering (under EUCC) kan ses som en endnu mere omfattende tredjeparts vurdering

Compliance muligheder

Basic products

- Module A
- Module B+C
- Module H
- EU Cybersecurity certification scheme

Important products Class I + RED DA

- Module A (Full hEN)
- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

Important products Class II

- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

Critical products

- EU Cybersecurity certification scheme (AL >= Substantial) for the specific product type
- As Class II, if no scheme exists

EN 18031-1

- Harmoniseret og citeret standard til RED DA art 3(3)(d) (Internetforbundet radioudstyr)

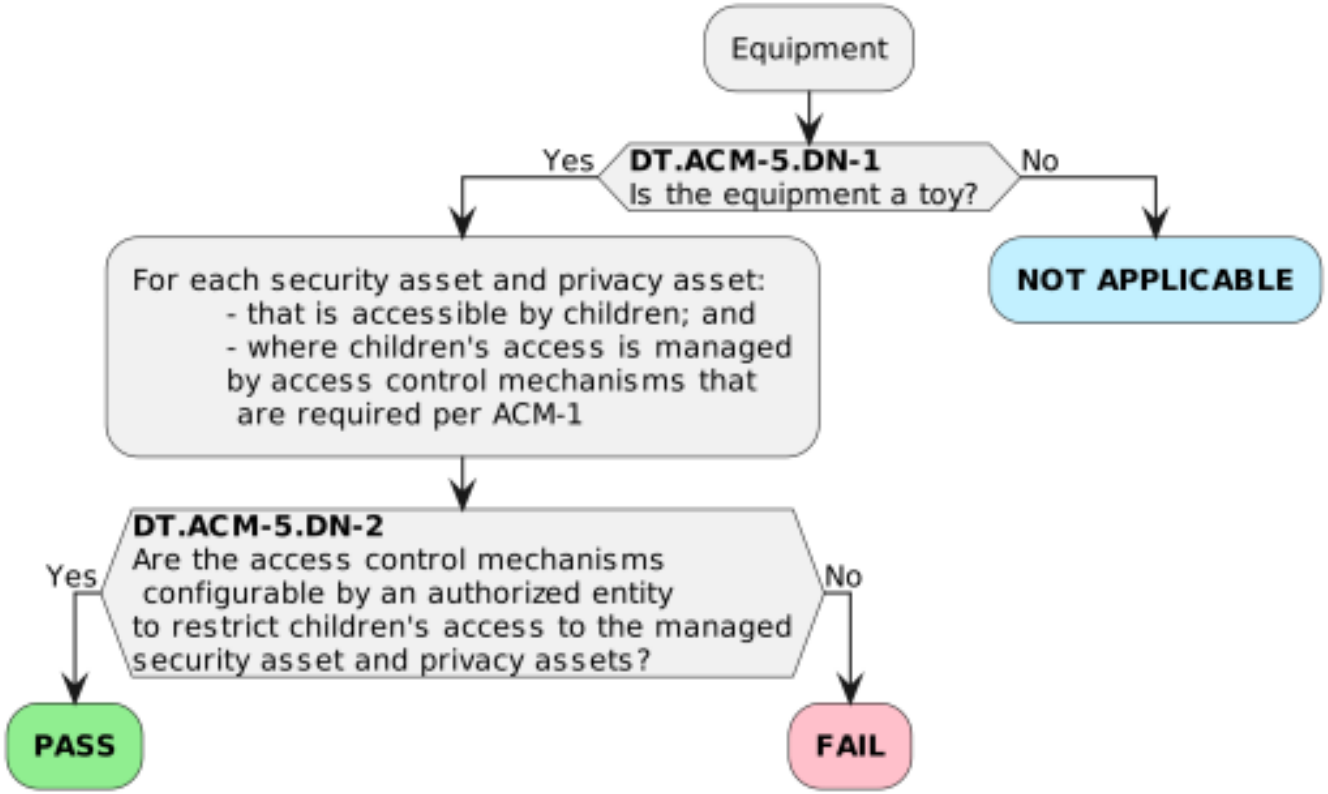
Generelle sikkerhedskrav til radioudstyr – Del 1: Radioudstyr med internetforbindelse

Common security requirements for radio equipment – Part 1: Internet connected radio equipment

- En række krav til produktet, f.eks autentifikation, software opdatering, sikker kommunikation og kryptografi
- Bygget op omkring beslutningtræer

- Gratis download i DS webshop (webshop.ds.dk)

EN 18031 beslutningstræer



Gode råd:

- ”Not applicable” kan indebære mindre arbejde end ”pass”
- Vær grundig med at få beskrevet alle assets/interfaces/osv.
- Har i flere lignende produkter, kan det være en god ide at genbesøge definitionerne af assets/software/hardware/osv., så man sikrer det ikke er for opsplittet

CRA – lidt mere kompleks

- RED DA kan kun stille krav til produktet, ikke processer
- CRA indeholder også proceskrav til sårbarhedshåndtering, ”security by design” og er risikobaseret

CRA standarderne

- 3 Horisontale (brede) standarder for alle produkter:
  - EN 40000-1-2: Sikker udvikling og risikovurdering
    - Måldato: December 2026
  - EN 40000-1-4: Tekniske sikkerheds mekanismer
    - Baseret på 18031, kommer i 2027
  - EN 40000-1-3: Sårbarhedshåndtering
    - Måldato: December 2026
    - Målet er at denne skal citeres mhp. formodningsret
- Derudover vertikale (smalle) standarder for produktkategorierne i Vigtig I, Vigtig II og Kritisk

Hvad kommer vi videre?

- Kig på EN 18031 – Det er ikke kun relevant ifbm. RED, da de tekniske krav er ca. de samme for CRA
  - Laver du radioudstyr, så fokuser primært på at kunne opnå compliance*
  - Identificeres større tekniske udfordringer, så fokuser på at få dem løst til CRA
- Få beskrevet jeres software udviklingsproces og få lavet en politik for sårbarhedshåndtering så i er klar til CRA
  - EN 40000-1-2 og -1-3 kan hjælpe med indholdet, men er endnu ikke færdige
  - Det er altid lettere at tage udgangspunkt i ”noget” end at starte fra bunden

- *Vi har et gratis værktøj til dokumentation, men det kræver kendskab til EN 18031. Vi er også DANAK akkrediteret til at udføre EN 18031-1 afprøvning af produkter

Kontakt

Michael Stausholm
Principal Security Architect

Michael.stausholm@alexandra.dk
20296322

ALEXANDRA INSTITUTTET