Cyber Resilience Act

ULVEN ER HER NÆSTEN

8/9-2026

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.

Cyber Resilience Act

– hvad er det

- En ny EU lov, der skal sikre cybersikkerhed i “Produkter med Digitale Elementer”
- Hidtil har området ikke været reguleret
  - En ny verden for alle
  - Kravene gælder i hele produktets levetid(!)
- Konsekvenser:
  - Forbud af salg / tilbagetrækning af produkter
  - Bøde op til 15 mio € eller 2.5% af samlet global omsætning

De vigtige datoer:

- Fuld effekt fra 11. december 2027:
  - Alle tekniske og process kravene i Bilag 1
- Indrapportering fra 11. september 2026:
  - Artikel 14:
    - Kendte og aktivt udnyttede sårbarheder i produktet
    - Hændelser der kan påvirke sikkerheden i produktet

Indrapportering af sårbarheder (Artikel 14)

- ”Bliver man bekendt med et angreb på et produkt man har solgt, skal det indrapporteres”
- Indrapportering til de nationale CSIRT (Styrelsen for Samfundssikkerhed)
  - Minder om tilsvarende krav i NIS 2 og GDPR
- I praksis:
  - Anvend ENISA portalen “Single Reporting Platform”

Indrapportering af sårbarheder (Artikel 14)

- 24-timer “early warning” rapport:
  - Produktnavn og producent
  - Medlemslande hvor produktet er tilgængeligt (!)
- 72-timer “fuld” rapport:
  - Foreløbig information om hændelsen
  - Foreløbige (mulige) mitigeringer
- Endelig afsluttet rapport
  - Detaljer om hændelsen
  - Detaljer om mitigeringer/sikkerhedsopdateringer

Hvad skal man ikke (endnu)

- Lidt forvirring/sammenblanding:
  - Process kravene i Bilag 1, Part 2 træder først i kraft i december 2027
- Man behøver derfor ikke (endnu) at have en politik for sårbarhedshåndtering, koordineret sårbarhedsafsløring, osv.
- Bliver man bekendt med en CVE i en komponent, skal det **ikke** indberettes
  - Med mindre I bliver opmærksomme på nogen eller noget udnytter sårbarheden i jeres produkt.

Bilag 1 kravene

Bilag 1 er delt i to:

- Del 1 med tekniske krav til produktet
  - Også inddirekte proceskrav: Risikovurdering og følge en sikker udviklingsproces for produktet.

- Del 2 med proces krav til sårbarhedshåndtering
  - Gælder i princippet for det enkelte produkt, men den samme process kan godt dække flere forskellige produkter

Del 1 (et lille uddrag)

Del I Cybersikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer

1) Produkter med digitale elementer skal designes, udvikles og produceres på en sådan måde, at de sikrer et passende cybersikkerhedsniveau baseret på risiciene.

2) På grundlag af den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2, og hvor det er relevant, skal produkter med digitale elementer:

   a) gøres tilgængelige på markedet uden kendte sårbarheder, der kan udnyttes

   b) gøres tilgængelige på markedet med en sikker konfiguration som standard, medmindre andet er aftalt mellem fabrikanten og erhvervsbrugeren i forbindelse med et skræddersyet produkt med digitale elementer, herunder muligheden for at nulstille produktet til dets oprindelige tilstand

   c) sikre, at sårbarheder kan afhjælpes gennem sikkerhedsopdateringer, herunder, hvor det er relevant, ved hjælp af automatiske sikkerhedsopdateringer, der som standardindstilling installeres, inden for en passende tidsramme, med en klar og brugervenlig fravalgsmekanisme og gennem underretning af brugerne om tilgængelige opdateringer og muligheden for midlertidigt at udsætte dem

   d) sikre beskyttelse mod uautoriseret adgang ved hjælp af passende kontrolmekanismer, herunder, men ikke begrænset til, autentificerings-, identitets- eller adgangsstyringssystemer, og give melding om mulig ikkeautoriseret adgang

   e) beskytte fortroligheden af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, såsom ved at kryptere relevante data i hvile eller i transit ved brug af mekanismer på det aktuelle tekniske niveau og ved brug af andre tekniske midler

   f) beskytte integriteten af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, kommandoer, programmer og konfigurationer mod enhver manipulation eller ændring, som brugeren ikke har givet tilladelse til, og give melding om korruption

Del 1 (Typiske udfordringer)

- Sårbarhedsscanning – ”Hvordan, hvornår, hvor ofte?”
- Sikkerhedsopdateringer – ”Vores produkt understøtter det ikke”
- Overvågning / logning – ”Det har vi ikke gjort hidtil”
- Data i produktet – ”Hvad skal/må vi indsamle/behandle?”

Del 2

Del II Krav til håndtering af sårbarheder

Fabrikanter af produkter med digitale elementer skal:

1) identificere og dokumentere sårbarheder og komponenter i produkter med digitale elementer, herunder ved at udarbejde en softwarekomponentliste i et almindeligt anvendt og maskinlæsbart format, der som minimum dækker de vigtigste produktafhængigheder

2) i forbindelse med risiciene forbundet med produkter med digitale elementer straks håndtere og afhjælpe sårbarheder, herunder ved at sørge for sikkerhedsopdateringer, og hvor det er teknisk muligt, skal nye sikkerhedsopdateringer leveres adskilt fra funktionalitetsopdateringer

3) anvende effektive og regelmæssige afprøvninger og gennemgange af sikkerheden af produktet med digitale elementer

4) når en sikkerhedsopdatering er gjort tilgængelig, dele og offentliggøre oplysninger om afhjulpne sårbarheder, herunder en beskrivelse af sårbarhederne, oplysninger, der gør det muligt for brugerne at identificere det berørte produkt med digitale elementer, sårbarhedernes indvirkning og alvor, og tydelige og tilgængelige oplysninger, der gør det lettere for brugerne at afhjælpe sårbarhederne; i behørigt begrundede tilfælde, hvor fabrikanterne mener, at sikkerhedsrisiciene ved offentliggørelse opvejer sikkerhedsfordelene, kan de udsætte offentliggørelsen af oplysninger om en afhjulpen sårbarhed, indtil brugerne har fået mulighed for at anvende den relevante rettelse

5) indføre og håndhæve en politik for koordineret offentliggørelse af sårbarheder

6) træffe foranstaltninger til at lette udvekslingen af oplysninger om potentielle sårbarheder i deres produkt med digitale elementer samt i tredjepartskomponenter indeholdt i det pågældende produkt, herunder ved at anføre en kontaktadresse til indberetning af de sårbarheder, der opdages i produktet med digitale elementer

7) sørge for mekanismer til sikker distribution af opdateringer for produkter med digitale elementer for at sikre, at sårbarheder afhjælpes eller afbødes rettidigt og, hvor det er relevant for sikkerhedsopdateringer, automatisk

8) sikre, at tilgængelige sikkerhedsopdateringer til afhjælpning af identificerede sikkerhedsproblemer formidles uden unødigt ophold og, medmindre andet er aftalt mellem en fabrikant og en erhvervsbruger i forhold til et skræddersyet produkt med digitale elementer, gratis sammen med vejledende meddelelser, der giver brugerne de relevante oplysninger, herunder om mulige foranstaltninger, der skal træffes.

Del 2 (Typiske udfordringer)

- Politikker / compliance – ”Vi har ikke noget skrevet ned”
- SBOM – ”Skal vi have styr på vores afhængigheder?”
- Afprøvninger / reviews – ”Hvor ofte og hvor grundige?”
- Transparens – ”Hvad skal vi dele med offentligheden?”

Dokumentation og compliance

CE-Mærkning

- Selvdeklarering: “overholder EU lovgivning”:
  - Selvevaluering: Hvilken lovgivning er produktet omfattet af
  - Vedligeholde teknisk dokumentation / teknisk fil
  - Markedsovervågningsmyndighed fører tilsyn og kigger på den tekniske dokumentation
  - Compliance krav til den tekniske dokumentation kan variere:
    - Selvevaluering (med metodefrihed)
    - Selvevaluering (baseret på en citeret harmoniseret standard)
    - Ekstern godkendelse ved bemyndiget organ (notified body)
    - Certificering

The Cyber Resilience Act

Annex III og IV: 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

Definition på Vigtig I, II og Kritiske produkter

- Pr. 28/11-2025: Implementing Act med beskrivelser

17.Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems	Products with digital elements that protect the physical security of consumers in a residential setting and which can be controlled or managed remotely from other systems, as well as hardware and software that centrally control such products. This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems and home security cameras.
12.Routers, modems intended for the connection to the internet, and switches	Routers are products with digital elements that establish and control the flow of data between different networks by selecting paths or routes using routing protocol mechanisms and algorithms, typically operating at the network layer. This category includes but is not limited to wired and wireless routers, virtual routers and routers with or without modems.
	Modems intended for the connection to the Internet are hardware products with digital elements that use digital modulation and demodulation techniques to convert analogue signals from and to digital signals for IP-based communication. This category includes but is not limited to fibre modems, Digital Subscriber

Standarder!

- Best practice
- Konkretiserer kravene i loven:

Fabrikanter af produkter med digitale elementer skal:

1) identificere og dokumentere sårbarheder og komponenter i produkter med digitale elementer, herunder ved at udarbejde en softwarekomponentliste i et almindeligt anvendt og maskinlæsbart format, der som minimum dækker de vigtigste produktafhængigheder

- Aldrig et lovkrav
  - Men det kan være det letteste / billigste alternativ

Relevante standarder

- EN 40000-1-x serien: Målrettet alle produkter under CRA
  - EN 40000-1-2: Principper for Cyber Resilience - Økosystem og sikker udvikling
  - EN 40000-1-3: Vulnerability handling – Proceskrav ifbm sårbarhedshåndtering
  - EN 40000-1-4: Generic Security Requirements – Tekniske produktkrav
- EN 62443-x serien: Målrettet industrielle produkter under CRA
  - Europæisk variant af IEC 62443 udviklet til CRA
  - 62443-4-1 om sikker udvikling og 62443-4-2 med tekniske produktkrav

COMING SOON

Relevante standarder – del 2

- Derudover en række produktkategori-specifikke standarder
  - Fra både ETSI og CEN/CLC
  - Nogle bygger videre på EN 40000 og 62443 serierne
  - Andre er ”uafhængige”

- En oversigt findes på stan4cra.eu

Next steps

- Er vi klar til at Artikel 14 træder i kraft på fredag?
  - Har vi overblik over hvilke lande vores produkter er tilgængelige i?
  - Hvordan afklarer vi om en hændelse skal rapporteres?
  - Hvem foretager indrapporteringen?
- Har vi en plan for kravene d. 11/12-2027?
  - Har vi lavet en overordnet gap-analyse mod kravene i Bilag I (både tekniske og proces krav)
  - Ved vi om vores produkter klassificeres som vigtige eller kritiske?
- Få beskrevet eksisterende software udviklings- og sårbarhedshåndterings-processer

- Kig på relevante standarder:
  - EN 40000 og EN 62443 når de kommer (evt. i kladde)
  - EN 18031, ISO 30111 og ISO 29147, ETSI 303 645,

Kontakt

Michael Stausholm
Principal Security Architect

Michael.stausholm@alexandra.dk
20296322

ALEXANDRA INSTITUTTET