Produkters Cybersikkerhed

Mette
Peetz-Schou
Dansk Standard den 5. oktober 2023

Dansk Industri

Cybersikkerhed

- Stort ønske om regulering blandt EU's medlemsstater
- EU har arbejdet på lovforslag længe

Indirekte krav via krav om produkters sikkerhed og frivillige certificeringsordninger

Direkte krav i mange forskellige produktlovgivninger med mange forskellige formål

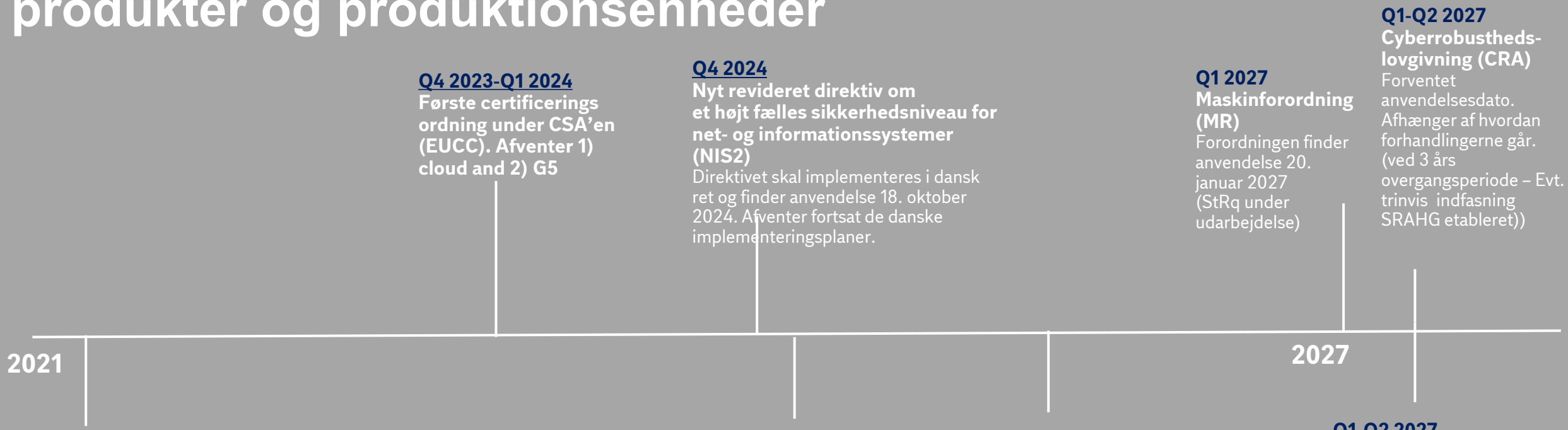
- Krigen i Ukraine har kun bestyrket EU i nødvendigheden af regulering – hurtigt!
- Fra sikring af det enkelte produkt til forsyningssikkerhed – større autonomi i Europa

Dansk Industri

Produktionsenheder	Produkter
Vigtige enheder under NIS2 f.eks. Produktion af Maskiner Elektronik og elektriske produkter Fødevarer Kemikalier (udvidet anvendelsesområde i forhold til NIS)	Maskinforordning
	Delegeret retsakt under radioudstyrsdirektivet
	Kunstig intelligens forordning
	Cyberrobusthed, inkl. stand alone software og services
Vigtige enheder under NIS2 f.eks. Produktion af medicinsk udstyr	Medicinsk udstyr og in vitro diagnostik
	Forbrugerprodukter (GPSD)
Cybersikkerhedscertificering (CSA)	

Dansk Industri

Anvendelsesdato for EU lovgivning vedr. cybersikkerhed - produkter og produktionsenheder



Q2 2021
Forordning om cybersikkerhed (CSA)
Forordningen fandt anvendelse den 28. juni 2021
Evaluering af forordningen er igangsat med offentlig høring (deadline 16. september 2023)

Q4 2023-Q1 2024
Første certificerings ordning under CSA'en (EUCC). Afventer 1) cloud and 2) G5

Q4 2024
Nyt revideret direktiv om et højt fælles sikkerhedsniveau for net- og informationssystemer (NIS2)
Direktivet skal implementeres i dansk ret og finder anvendelse 18. oktober 2024. Afventer fortsat de danske implementeringsplaner.

Q4 2024
Forordning om produkters sikkerhed i almindelighed (GPSR). Finder anvendelse 13. december 2024. Vil medfører ændringer i den danske lov om produkter (der bl.a. implementerer markedsovervågnings-forordningen (EU)1020/2019.

Q3 2025
Kommissions forordning under Artikel 3.3 i Radioudstyrsdirektivet (RED)
Forordningen finder anvendelse 1. august 2025.
(Standardiser i høring pt.)

Q1 2027
Maskinforordning (MR)
Forordningen finder anvendelse 20. januar 2027
(StRq under udarbejdelse)

Q1-Q2 2027
Cyberrobustheds-lovgivning (CRA)
Forventet anvendelsesdato. Afhænger af hvordan forhandlingerne går. (ved 3 års overgangsperiode – Evt. trinvis indfasning SRAHG etableret))

Q1-Q2 2027
Forordning om kunstig intelligens (AIR)
Forventet anvendelsesdato. Afhænger af hvordan forhandlingerne går.
(ved 3 års overgangsperiode)

Dansk Industri

Forordning om (forbruger)produkters sikkerhed i almindelighed (GPSR)

Artikel 5

Almindeligt sikkerhedskrav

Erhvervsdrivende må kun bringe sikre produkter i omsætning eller gøre sikre produkter tilgængelige på markedet.

Artikel 6

Aspekter til vurdering af produkters sikkerhed

1. I forbindelse med vurdering af, hvorvidt et produkt er sikkert, tages der navnlig hensyn til følgende aspekter:

g) når produktets art kræver det, de passende egenskaber hvad angår cybersikkerhed, som er nødvendige for at beskytte produktet mod påvirkninger udefra, herunder ondsindede tredjemænd, hvis en sådan påvirkning kan have indflydelse på produktets sikkerhed, herunder et muligt tab af indbyrdes sammenhæng

Dansk Industri

(EU) 2023/988

Produkter omfattet af kravet

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på produkter, som bringes i omsætning eller gøres tilgængelige på markedet, medmindre der findes EU-ret med specifikke bestemmelser om sikkerheden ved de pågældende produkter, som har samme formål.

Når produkter er omfattet af specifikke sikkerhedskrav ifølge EU-retten, finder denne forordning kun anvendelse på de aspekter og de risici eller kategorier af risici, som ikke er omfattet af disse krav.

I denne forordning forstås ved:

1) »produkt«: ethvert produkt, som, hvad enten det har forbindelse med andre varer, der mod eller uden vederlag leveres eller gøres tilgængelige, herunder i forbindelse med levering af en tjenesteydelse, eller ej, er bestemt for forbrugerne, eller som under rimeligt forudsigelige betingelser sandsynligvis vil blive anvendt af forbrugerne, selv om det ikke er bestemt for dem

Radioudstyrs cybersikkerhed

- Skal sikrer, at radioudstyr
  - Ikke skader nettet eller dets funktion eller misbruger net ressourcer på en sådan måde, at det medfører en uacceptabel forringelse af tjenesten.
  - Er i stand til at sikre, at personoplysninger om brugeren og abonnenten og disses privatliv beskyttes
  - Understøtter visse faciliteter, der sikrer beskyttelse mod svig

- Gælder for radioudstyr, der kan forbindes til internettet
  - Direkte eller indirekte kommunikation via andet udstyr
    - Legetøj, børneprodukter, kropsbåret udstyr mv. i fokus under forhandlinger (forbrugerbeskyttelse)
    - Rammer alt – også industriel anvendelse af radioudstyr

Dansk Industri

Hvad betyder det i praksis?

Harmonised standards in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:

d	1.	include elements to monitor and control network traffic, including the transmission of outgoing data;
d	2.	is designed to mitigate the effects of ongoing denial of service attacks;
def	3.	implement appropriate authentication and access control mechanisms;
def	4.	are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the <d><e><f>;
def	5.	are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to <d><e><f>;
def	6.	protect the exposed attack surfaces and minimise the impact of successful attacks.
ef	7.	protect stored, transmitted or otherwise processed <e> <f> against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e> <f>;
e	8.	include functionalities to inform the user of changes that may affect data protection and privacy;
ef	9.	log the internal activity that can have an impact on <e> <f>;
e	10.	allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information;

<d> = network or its functioning or misuse of network resources, <e> = personal & location data protection and privacy, <f> = financial or monetary data

Regelefterlevelse I

- Direktivet om radioudstyr bygger på New Legislative Framework
- De tekniske specifikationer udvikles i form af harmoniserede standarder, der publiceres i EU-Tidende (hEN)
  - Efterlevelse af de publicerede standarder (hEN) giver formodningsret og fri bevægelighed af produkter i EU

Dansk Industri

Regelefterlevelse II

- Hvis der ikke findes publicerede harmoniserede standarder (hEN) skal et bemyndiget organ involveres i overensstmmelsesvurderingen
  - EU-typeafprøvning efterfulgt af typeoverensstemmelse på grundlag af intern produktionskontrol
  - Overensstemmelse på grundlag af fuld kvalitetssikring

- Vigtigt at standarderne bliver færdige og publiceret til tiden
- Standarderne er i høring nu – vigtigt at forholde sig til dem

- Skal implementeres før 1. august 2025, hvor reglerne finder anvendelse

Dansk Industri

Maskinforordningen

1.1.9. *Beskyttelse mod forvanskning*

Maskinen eller det relaterede produkt skal konstrueres og fremstilles således, at dets forbindelse til en anden anordning, ved selve den tilsluttede anordnings egenskaber eller ved enhver anordning, som er fjerntilsluttet maskinen eller det relaterede produkt, ikke fører til farlige situationer.

En hardwarekomponent, som transmitterer signaler eller data, som er relevante for forbindelse eller adgang til software, der er kritisk for maskinen eller det relaterede produkts overensstemmelse med de relevante væsentlige sikkerheds- og sundhedskrav, skal fremstilles således, at den er tilstrækkeligt beskyttet mod tilsigtet eller utilsigtet forvanskning. Maskinen eller det relaterede produkt skal indsamle dokumentation for legitim eller illegitim indtrængen i denne hardwarekomponent, når det er relevant for forbindelse eller adgang til software, der er kritisk for maskinens eller det relaterede produkts overensstemmelse med kravene.

Software og data, der er kritisk for maskinens eller det relaterede produkts overensstemmelse med de relevante væsentlige sikkerheds- og sundhedskrav, skal identificeres som sådan og skal være tilstrækkeligt beskyttet mod tilsigtet og utilsigtet forvanskning.

Maskinen eller det relaterede produkt skal identificere softwaren, der er installeret i dem, og som er nødvendig for en sikker drift, og de skal til enhver tid være i stand til at forelægge disse oplysninger i et lettilgængeligt format.

Maskinen eller det relaterede produkt skal indsamle dokumentation for legitim og illegitim indtrængen i software, eller en ændring i den i maskinen eller det relaterede produkt installerede software eller dens konfiguration.

Maskinforordningen, fortsat

1.2.1. *Styresystemernes sikkerhed og pålidelighed*

Styresystemerne skal være konstrueret og fremstillet således, at der ikke kan opstå farlige situationer.

Styresystemer skal være konstrueret og fremstillet således:

a) at de efter omstændighederne og risiciene kan modstå de tilsigtede driftspåvirkninger og tilsigtede og utilsigtede ydre påvirkninger, herunder tredjeparters ondsindede handlinger, som med rimelighed kan forudses, og som fører til en farlig situation

Standardiseringsanmodningen er under udarbejdelse nu

Produkter med digitale elementers cyberrobusthed

- Lovgivning baseret på New Legislative Framework(NLF)
- Ryde op i den fragmenterede tilgang til regulering af cybersikkerhed

- Lovforslag stadig under forhandling i EU (forventes afsluttet i år)
  - Vi kender ikke de endelige krav endnu!

- Krav til flere produkter
  - Ikke kun fysiske produkter, også software og udvalgte services
- Krav gennem hele produktets livscyklus
  - Support periode

- Minimumslovgivning for cybersikkerhed (som GPSR for sikkerhed)
  - Samme krav til alle produkter, når relevant i forhold til risikovurderingen

Hvilke krav stilles?

- Krav til selve produktet, inkl. dokumentation af udviklingsfasen (SBOM) og løbende risikovurdering
  - Bygger ovenpå kravene i Kommissionsforordningen under radioudstyrsdirektivet

- Krav til håndtering af sårbarheder
  - Gratis softwareopdateringer

- Krav til rapportering af aktivt udnyttede sårbarheder og alle hændelser
  - Ikke håndterede sårbarheder og proportionalitet af krav er til diskussion
  - Forsøg på tilretning af kravene til NIS2, når det gælder tidsfrister, definitioner mv.
  - Nationale CSIRT eller ENISA, som modtager af rapporteringerne
    - Vigtigt at rapportering kun skal ske ét sted, i ét format på ét sprog

Kategorisering af produkter efter risiko

- Kategorisering har betydning for hvem der kan udføre overensstemmelsesvurderingen

- Kritisk 1 kræver brug af notificeret organ, hvis der ikke findes hEN
- Kritisk 2 kræver brug af notificeret organ
- (Kritisk 3 stiller krav om certificering)
  - Forslag fra Rådet dvs. medlemsstaterne
  - Bryder med princippet om ”minimumslovgivning” og NLF-principper
- Fabrikanten kan benytte modul A for alle andre produkter
  - Denne kategori bør være så bred som mulig

- Forventer at reglerne finder anvendelse 36 måneder efter, at forordningen træder i kraft

Dansk Industri

SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

Made avaliable/ placed on the market

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

Produktkrav vedr. cybersikkerhed (fortsat)
Hvis relevant i forhold til risikovurderingen.

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

Håndtering af sårbarheder

VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Standarder under Cyberrobusthedslovgivningen

- Standardisation Request Ad Hoc Group (SRAHG) er etableret
- Udkast til standardiseringsanmodning i høring i CEN/CENELEC
- Der lægges op til +40 standarder
  - Urealistisk

- Behov for realistisk tidsplan for udviklingsprocessen
- Anvend eller byg videre på eksisterende standarder
- Prioriter de områder, hvor der ikke findes standarder
- Sikre internationalt samarbejde
- Fokus på at udvikle objektive testmetoder

Konklusion

- Mange nye regler vedr. produkters cybersikkerhed på vej
- Nødvendigt at forholde sig til dem nu
- Arbejd med produkternes cybersikkerhed samtidigt med cybersikkerheden af produktionsenheden (NIS2)
  - Skel til Cyberrobusthedsforordningen, selvom det ikke er de regler, der skal anvendes først
    - Reglerne vedr. Radioudstyr forventes at blive trukket tilbage,
    - Relationen til anden cyberlovgivning er stadig uklar
  - Overvej NIS2 krav, også selvom I ikke bliver omfattet
    - Cybertruslen er reel og kan lægge jeres forretning ned
  - Se om D-mærket kan hjælpe jer på vej
    - D-mærket | Mærkningsordning for it-sikkerhed og data (d-maerket.dk)
  - Kom på forkant gennem deltagelse i standardisering (S-441) og bidrag til høringen om RED-standarderne
  - Søg inspiration i DS/PAS 2600:2021 (cybersikkerhed i produkter (IoT))
- Lovgivningen introduceres løbende
  - Designfasen, når det enkelte produkt bringes i omsætning og efter, at det er bragt i omsætning
- Krav om processer på tværs af udvikling, regelefterlevelse, legal, IT og OT er en udfordring

Hvis I har spørgsmål

Mette Peetz-Schou
Seniorchefkonsulent,
Europapolitik
Dansk Industri

Phone: 33773022
Mobile: 40373728
Mail: meps@di.dk

Dansk Industri