Få styr på EU's cybersikkerhedskrav

Lancering af en praktisk guide til SMV'er

10. december 2024

Alexandra Instituttet
Force Technology
Dansk Standard

Hvad har vi med til jer i dag?

- Introduktion til guiden
- Cybersikkerhed i en SMV-kontekst – udgangspunkt i NIS2 og CRA
- Mulighed for at stille spørgsmål

Om Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 190 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

Dansk Standard har gode erfaringer med at udvikle guides, der hjælper virksomheder med at forstå og arbejde med standarder

Formål med guiden

DS DANSK STANDARD

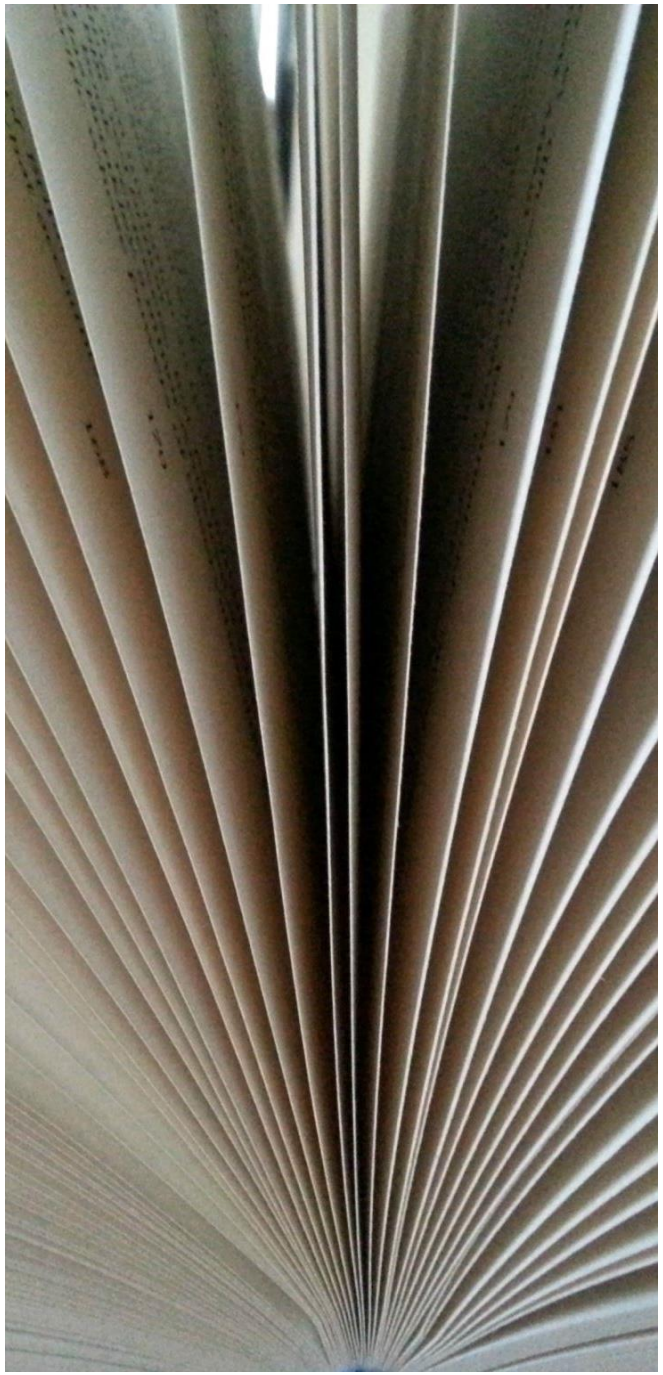
- Hjælpe SMV'er med at få et overblik over EU's lovkrav på cybersikkerhedsområdet
- Introducere lovtekster (Cyber Resilience Act og NIS2-direktivet) på en overskuelig måde
- Give inspiration til at gribe arbejdet an og udarbejde en strategi for cybersikkerhed
- Præsentere værktøjer der kan lette arbejdet for SMV'er – anvendelsen af standarder

Hent guiden her:
https://www.ds.dk/da/download/ds-inf-21007-2024

Baggrund for guiden

Cyber- og informationssikkerhed er en del af EU's digitale strategi. Danske virksomheder og organisationer skal forholde sig til en del lovgivning på cyberområdet:

- **NIS2**
- **Cyber Resilience Act**
- Radioudstyrsdirektivet (RED DA) – cybersikkerhedskrav
- Cyber Security Act - frivillig certificeringsordning. Der arbejdes pt. på tre certification schemes: EUCC (common criteria), EUCS (cloud) og EU5G (5G)
- Cyber Solidarity Act
- DORA



Guidens indhold

- **Introduktion til lovkrav på cyberområdet**
  - Koblingen mellem standarder og lovgivning
  - Introduktion til CE-mærkning

- **Introduktion til Cyber Resilience Act og NIS2-direktivet**
  - Baggrund og formål
  - Krav
  - Målgruppe
  - Koblingen til standarder
  - SMV perspektiv
  - Konkrete eksempler

- **Anneks**
  - AI Act
  - Radio Equipment Directive (RED) – Delegated Acts
  - Revised Product Liability Directive
  - General Product Safety Regulation (GPSR)
  - Machinery regulation
  - Cyber Security Act
  - Cyber Solidarity Act

Guiden anvender tre virksomhedseksempler

En softwarevirksomhed med otte ansatte, hvis primære produkt er en app til smartphones. Begrænset erfaring med cybersikkerhed

En virksomhed med 35 ansatte som producerer robotplæneklippere. Begrænset erfaring med cybersikkerhed

Et stort elselskab med ca. 1.200 ansatte der leverer strøm til ca. 100.0000 husstande. Leverer udover el også (fiber-)internet og installerer varmepumper samt ladestandere til elbiler. Arbejder systematisk med cybersikkerhed.

NIS2 og CRA

Jeppe Pilgaard Bjerre

NIS2 - overordnet

- politikker for **risikoanalyse** og informationssikkerhed
- håndtering af hændelser
- **driftskontinuitet** (back-up) og **krisestyring**
- **forsyningskædesikkerhed**, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører og tjenesteudbydere
- sikkerhed i forbindelse med **erhvervelse**, **udvikling** og **vedligeholdelse** af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
- politikker og procedurer til **vurdering af effektiviteten** af foranstaltninger til **styring af cybersikkerhedsrisici**
- grundlæggende **cyberhygiejnepraksisser** og **uddannelse** i cybersikkerhed
- politikker og procedurer ift. brug af kryptografi og, hvor det er relevant, kryptering
- **personalesikkerhed**, politikker for adgangskontrol og forvaltning af aktiver
- brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation samt sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant

NIS2

Se på virksomhedens størrelse.
Er I mere end 50 ansatte og en omsætning/balance på over 10 mio. €?

Under 50 ansatte eller omsætning under 10 mio. €

Kig i bilag 1 og 2. Hvis virksomhedens branchekode (NACE) er oplistet, er virksomheden omfattet af NIS2 forudsat et af følgende kriterier er opfyldt:

- Virksomheden er defineret som kritisk i forbindelse med CER-direktivet.
- Virksomheden leverer offentligt tilgængelige kommunikationsnetværk, trust tjenester eller DNS.
- Virksomheden er den eneste udbyder af en tjeneste som er kritisk for aktiviteter i samfundet eller økonomien.
- Afbrydelser af virksomhedens tjenester kan medføre betydelige konsekvenser for sundheden/sikkerheden i samfundet.
- Afbrydelser af virksomhedens tilbudte tjeneste kan medføre systemiske (evt. grænseoverskridende) risici.
- Virksomhedens tjeneste er kritisk for en specifik sektor eller branche.

Over 50 ansatte og omsætning over 10 mio. €

Kig i bilag 1 og 2. Hvis virksomhedens branchekode (NACE) er oplistet, er virksomheden omfattet af NIS2.

FORCE TECHNOLOGY

CRA - Overordnet

Regler for tilgængeliggørelse på markedet af produkter med digitale elementer

Væsentlige cybersikkerhedskrav til design, udvikling og produktion af produkter

Regler om markedsovervågning

Væsentlige cybersikkerhedskrav til sårbarhedshåndteringsprocesser,

CRA – Produkt typer

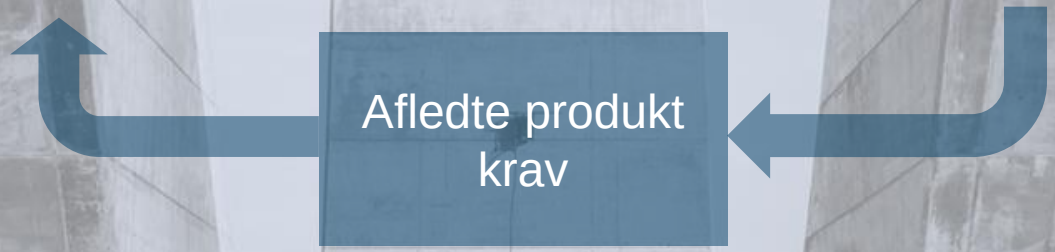
90 % af produkter	10 % af produkter		
Uden for produkt-kategori	**Vigtig Klasse I**	**Vigtig Klasse II**	**Kritisk**
Selv-evaluering	Harmoniseret standard eller tredjepartsvurdering	Tredjepartsvurdering	Obligatorisk EU-certificering
Kriterier n/a	Kriterier • Funktionalitet: Kritisk software • Type: Operativsystem, antivirus • Andet: Højrisiko		Kriterier Specifik produkttype
	Kan tilføjes/specificeres gennem delegeret retsakt		
Eksempler: Fotoredigering, tekstbehandling, smarte højtalere, diskdrev, spil	**Eksempler:** Password managers, netværksinterfaces, operativsystemer	**Eksempler:** Firewalls, virtualiseringssystemer, tamperproof microcontrollere	**Eksempler:** Smartcards, sikkerhedsbokse

CRA v. NIS2

	CRA	NIS2
Genstand	regler for tilgængeliggørelse på markedet af produkter med digitale elementer for at sikre cybersikkerheden for sådanne produkter	Dette direktiv fastlægger foranstaltninger, der sigter på at opnå et højt fælles cybersikkerhedsniveau i hele Unionen med henblik på at forbedre det indre markeds funktion.
Område	Produkter med digitale elementer	Organisationer
Krav	Produktkrav og udvikling	Strategier og politikker

CRA v. NIS2

	CRA	NIS2
Genstand	regler for tilgængeliggørelse på markedet af produkter med digitale elementer for at sikre cybersikkerheden for sådanne produkter	Dette direktiv fastlægger foranstaltninger, der sigter på at opnå et højt fælles cybersikkerhedsniveau i hele Unionen med henblik på at forbedre det indre markeds funktion.
Område	Produkter med digitale elementer	Organisationer
Krav	Produktkrav og udvikling	Strategier og politikker



NIS2 – Leverandørhåndtering - Guide

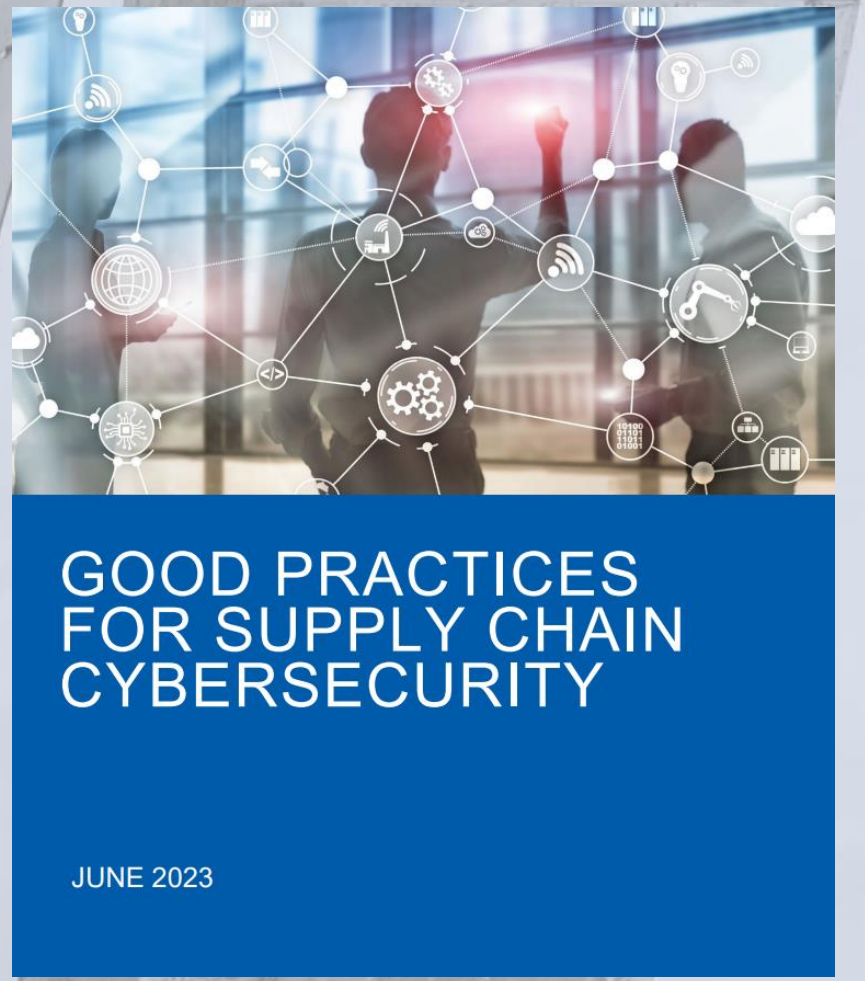
ENISA Publikation
LINK

Vejledning omkring krav til leverandøre til NIS2 omfattede enheder.

ISO/IEC 27001
ISO 9001

IEC 62443-4-1
IEC 62443-4-2

CRA (Næsten)



EU's Cybersikkerhedskrav

HVAD GØR VI SÅ I PRAKSIS?

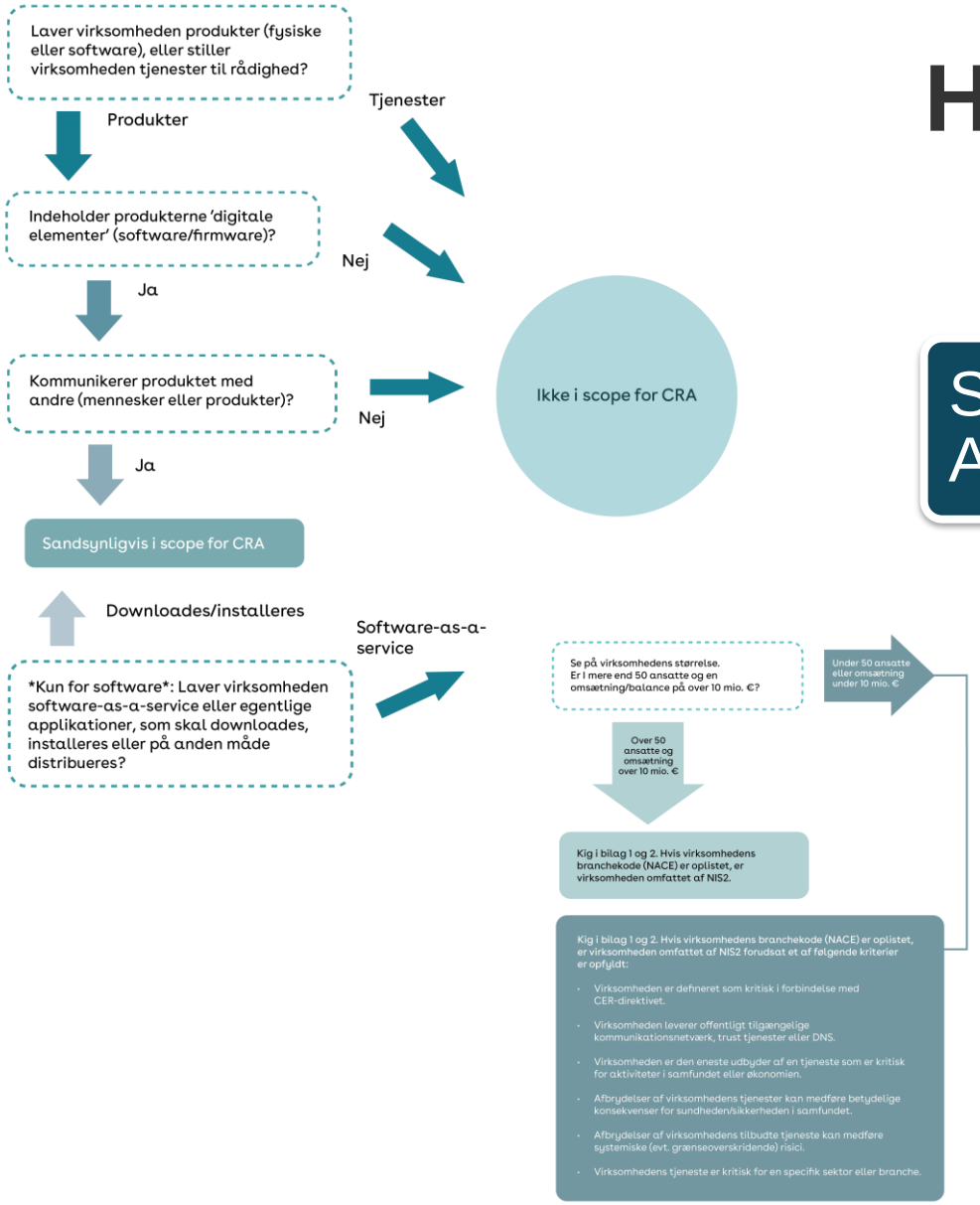
MICHAEL STAUSHOLM

PRINCIPAL SECURITY ARCHITECT

Hvad skal vi gøre?

- Hvilke love er relevante for os?
- Hvilke krav skal vi leve op til?
- Hvad gør vi allerede?
- Hvad mangler vi?

Hvilke love er relevante?



Særlig lovgivning (Medico, Automobiler, Finans, ?)

NIS 2 (direkte)

NIS 2 (underleverandør)

Produkt lovgivning (CRA)

Hvor findes kravene?

- Lovteksterne er tilgængelige (links i guiden)
  - NIS 2 Artikel 21
  - CRA Annex 2

- **NIS 2 underleverandør - tal med kunden**

NIS 2

Kravene
• a) politikker for risikoanalyse og informationssystemsikkerhed • b) håndtering af hændelser • c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring • d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere • e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder • f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici • g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse • h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering • i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver • j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

NIS 2 – Den simple udgave

Kravene

1. Formuler en sikkerhedspolitik (f.eks. Sikkerdigital.dk)
2. Overblik over vigtige systemer / informationer
3. En plan i tilfælde af at vi bliver angrebet
4. Screenings process i forbindelse med underleverandører

CRA: Kravene

Del I Cybersikkerhedskrav vedrørende egenskaberne ved 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
- g) kun behandle personoplysninger eller andre data, der er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til det tilsigtede formål med produktet med digitale elementer (»dataminimering«)
- h) beskytte tilgængeligheden af væsentlige og grundlæggende funktioner, også efter en hændelse, herunder gennem modstandsdygtigheds- og afbødningsforanstaltninger mod denial of service-angreb
- i) minimere den negative indvirkning af selve produkterne eller forbundne enheder på tilgængeligheden af tjenester, der leveres af andre enheder eller netværk
- j) designes, udvikles og produceres med henblik på at begrænse angrebsflader, herunder eksterne grænseflader
- k) designes, udvikles og produceres med henblik på at mindske virkningen af en hændelse ved hjælp af passende mekanismer og teknikker til begrænsning af udnyttelsen
- l) levere sikkerhedsrelaterede oplysninger ved at registrere og overvåge relevante interne aktiviteter, herunder adgang til eller ændring af data, tjenester eller funktioner, med en fravalgsmekanisme for brugeren
- m) give brugerne mulighed for på sikker og nem vis at fjerne alle data og indstillinger på permanent basis og, hvis sådanne data kan overføres til andre produkter eller systemer, sikre, at dette gøres på en sikker måde.

Del II Krav til håndtering af sårbarheder

- 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.

CRA: Kravene (forsimplet)

Del I Cybersikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer

- Lav en sårbarhedsscanning (periodisk og før release)
- Sørg for standard konfigurationen er “sikker”
- Understøt (sikkerheds) opdateringer, helst automatisk
- Implementer adgangskontrol (hvor relevant)
- Krypter data (fortrolighed og integritet) (hvor relevant)
- Minimer data indsamling/behandling til det nødvendige
- Beskyt essential/fundamental funktionalitet (resiliens)
- Minimer negativ konsekvens for andre produkter (i tilfælde af angreb)
- Minimer angrebsfladen og konsekvens i tilfælde af angreb
- Log og overvåg aktivitet
- Understøt sikker sletning (og migrering) af bruger data

Del II Krav til håndtering af sårbarheder

- Vedlighold en liste af brugte komponenter (dependencies)
- Understøt (sikkerheds) opdateringer, helst automatisk
- Udfør (sikkerheds) tests (og reviews)

Prioritering

Rød	Gul	Grøn
• Vi opfylder ikke kravet • Begynd implementering med det samme – kræver større ændringer	• Vi opfylder delvist kravet • Sammenhold med **eksisterende** best practice / standarder	• Vi opfylder kravet • Afvent endelig conformance formalia (f.eks harmoniseret standard)

Tid til spørgsmål

Koblingen mellem lovgivning på det digitale område og standarder

Cyber Resilience Act

Cyber Resilience Act er en ny EU-forordning som stiller fælleseuropæiske cybersikkerhedskrav til produkter med digitale elementer. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til de horisonale cybersikkerhedskrav.

Cyber Security Act

Den europæiske forordning om cybersikkerhed har til formål at etablere en fælles europæisk ramme for certificering inden for cybersikkerhed, som forventes at bygge på eksisterende standarder.

Data Act

Dataforordningen (Data Act) skal skabe harmoniserede regler om fair adgang til og anvendelse af data og gøre det lettere for europæiske virksomheder at dele og anvende data.

AI Act

Forordningen om kunstig intelligens (AI Act) skal sikre fælles spilleregler for brugen og udviklingen af kunstig intelligens. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til kravene om kunstig intelligens, som forordningen stiller.

Data Governance Act

Datastyringsforordningen (Data Governance Act) har til formål at skabe tillid til datadeling til gavn for samfundet, og der skal bl.a. prioriteres tværsektorielle standarder for datadeling og interoperabilitet.

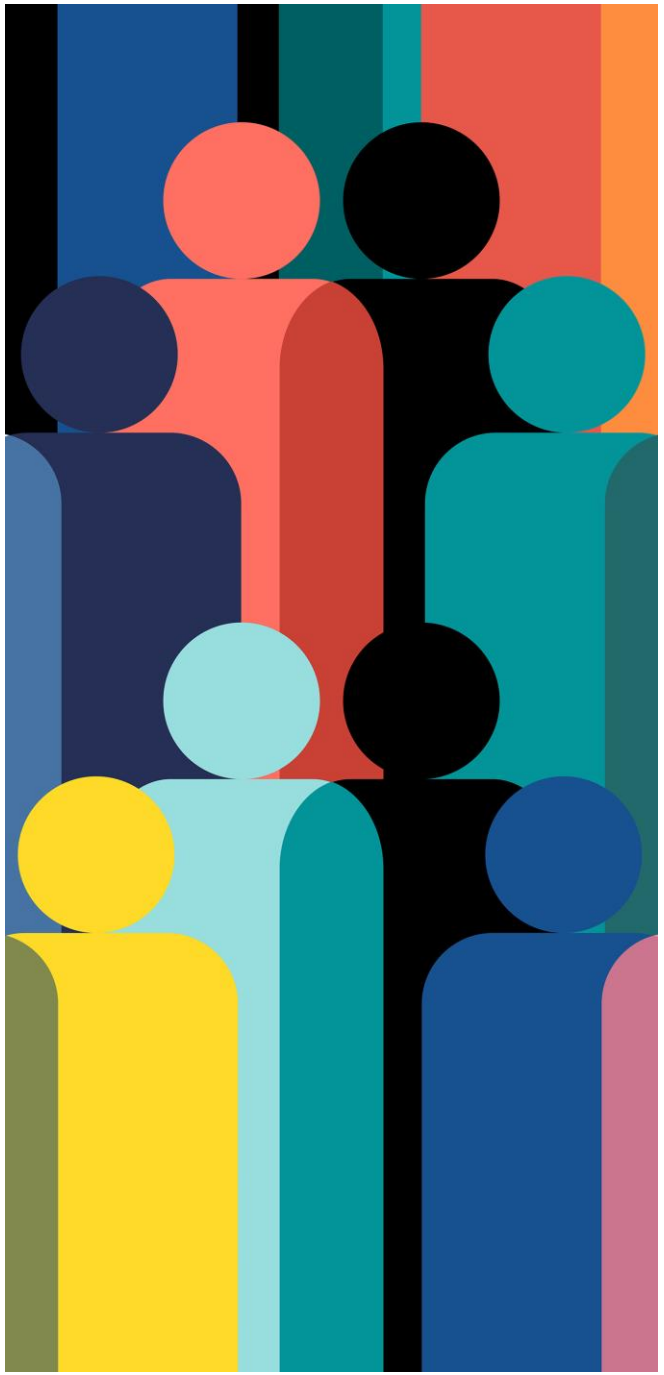
GDPR

Databeskyttelsesforordningen (GDPR) fastlægger fælleseuropæiske retningslinjer for håndteringen af personoplysninger for virksomheder, organisationer, myndigheder mm.

NIS2-direktivet

NIS2-direktivet indeholder skærpede krav til cyber- og informationssikkerhed i forhold til kritisk infrastruktur. Direktivet opfordrer til at anvende internationale, anerkendte standarder.

https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digitale-omraade-og-standarder



Workshop i Danmark om Cyber Resilience Act

- Planlagt til april 2025
- Finansieret af Kommissionen
- Workshoppen vil blive afholdt af Dansk Standard
- Workshoppen vil have fokus på 1 & 15 i Standardiseringsanmodningen

1.	European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
15.	European standard(s) on vulnerability handling for products with digital elements	30/08/2026

- Lignende workshops vil blive planlagt i Spanien og Cypern
- Målet er at få input til indholdet af standarderne fra fageksperter

Hvorfor arbejde med cybersikkerhed?

- Lovgivning
- Krav fra samarbejdspartnere/leverandører
- Styrket konkurrenceevne
- Systematisering af interne processer
- Opretholde kunders tillid
- Nye forretningsmuligheder

Husk at det er mere end blot en compliance øvelse!!

DANSK STANDARD