

Få styr på EU's cybersikkerhedskrav

– En praktisk guide til SMV'er



DANSK STANDARD

Få styr på EU's cybersikkerhedskrav - En praktisk guide til SMV'er

© Dansk Standard 2024

Kopiering ikke tilladt uden særlig tilladelse

DS/INF 21007:2024

Projektnummer: M389232

Tryk: Dansk Standard

Udgivet 2024

1. udgave

Udgivet af Dansk Standard

Göteborg Plads 1

2150 Nordhavn

Telefon: 39 96 61 01

ds@ds.dk

www.ds.dk

Dette er en POD-publikation

Printet i Danmark

Billeder: iStock og Unsplash

Guiden er udarbejdet af Alexandra Instituttet, Force Technology og Dansk Standard



Indholdsfortegnelse

Forord.....	4
Indledning	5
Hvordan skal guiden anvendes?	5
Præsentation af anvendte eksempler.....	6
Introduktion til lovkrav på cyberområdet	8
Koblingen mellem standarder og lovgivning	9
Introduktion til CE-mærkning.....	9
Cyber Resilience Act.....	12
Baggrund og formål	12
Hvad er kravene?	13
Hvem gælder lovgivningen for?.....	13
Koblingen til standarder	14
Hvilke krav skal SMV'erne forholde sig til?	15
Eksemplerne	17
NIS2-direktivet	20
Baggrund og formål	20
Hvad er kravene?	22
Hvem gælder lovgivningen for?.....	23
Koblingen til standarder	23
Hvilke krav skal SMV'erne forholde sig til?	26
Eksemplerne	28
Opsamling.....	29
Anneks	30
AI Act (AI-forordningen)	30
Radio Equipment Directive (RED) – Delegated Acts (Radioudstyrsdirektivet – delegerede retsakter).....	31
Revised Product Liability Directive (Direktivet om produktansvar).....	32
General Product Safety Regulation (GPSR) (Forordningen om produktsikkerhed i almindelighed).....	32
Machinery regulation (Forordningen om maskiner).....	32
Cyber Security Act (CSA) (Forordningen om cybersikkerhed)	33
Cyber Solidarity Act (Forordningen om cybersolidaritet).....	33
Bibliografi	34

Forord

Denne guide er udarbejdet i et samarbejde mellem Alexandra Instituttet, Force Technology og Dansk Standard. Guiden er udviklet i regi af Dansk Standards udvalg for cyber- og informationssikkerhed med støtte fra Erhvervsstyrelsen. Ambitionen er, at guiden kan bidrage til at klæde danske SMV'er på til at håndtere de kommende lovkrav fra EU i forhold til cyber- og informationssikkerhed.

Indledning

I en stadig mere digitaliseret verden er cybersikkerhed blevet en kritisk faktor for alle virksomheder uanset størrelse og branche. Men mens de større virksomheder ofte har ressourcerne til at systematisere arbejdet med cybersikkerhed, kæmper de små og mellemstore virksomheder (SMV'er) med begrænsede budgetter, manglende ekspertise og ikke mindst en stigende mængde lovkrav på området.

De skærpede lovkrav på cyberområdet er en del af EU's digitale strategi, der sigter mod at sikre Europas digitale suverænitet, styrke europæiske virksomheders modstandsdygtighed og skabe et sikkert digitalt EU.

Med strategien følger en række initiativer og konkrete krav til cybersikkerhed, som kommer til at påvirke en lang række danske virksomheder. Det gælder både virksomheder, der ikke traditionelt har haft stort fokus på cybersikkerhed, og virksomheder, der ikke direkte er omfattet af lovgivning. Det kan være virksomheder, hvor deres rolle som leverandør eller samarbejdspartner betyder, at der også vil være indirekte krav til dem.

Det bliver primært NIS2-direktivet¹ og Cyber Resilience Act², der kommer til at sætte dagsordenen for danske virksomheder i de kommende år, og derfor fokuserer denne guide også på dem.

Formålet med NIS2-direktivet er at skærpe cybersikkerheden i vigtige dele af samfundet og de omkringliggende forsyningsskæder. Konkret betyder det, at de virksomheder, der er omfattet, skal leve op til en række minimukrav, hvilket bl.a. involverer risikostyring og leverandørstyring. Det betyder også, at virksomheder, der ikke direkte er omfattet af loven, også kan blive omfattet af cybersikkerhedskrav via deres kunder.

Cyber Resilience Act derimod er specifikt rettet mod cybersikkerhed i digitale produkter, herunder både hardware og software. Lovgivningen kommer til at ramme bredt, da flere og flere produkter indeholder digitale elementer. I forbindelse med Cyber Resilience Act vil der blive udarbejdet standarder, der skal gøre det lettere for virksomhederne at leve op til lovgivningen. Standarderne kommer til at indeholde konkrete retningslinjer for sårbarhedshåndtering, secure by design/default osv.

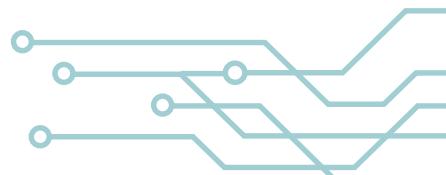
Begge lovgivningsområder uddybes yderligere i guiden.

Hvordan skal guiden anvendes?

Denne guide er designet til at hjælpe SMV'er med at navigere i det komplekse landskab af cybersikkerhed og de europæiske lovkrav. Guiden giver en introduktion til de væsentligste lovkrav på cyberområdet – særligt NIS2-direktivet og Cyber Resilience Act³ – som kommer til at have stor indflydelse på danske virksomheder i de kommende år.

Formålet med guiden er at give danske SMV'er inspiration og gode værktøjer til at komme i gang med at udarbejde en strategi for cybersikkerhed. Strategien skal sikre, at virksomheder har taget stilling til de kommende lovkrav.

Da lovkravene er komplekse, kan det være vanskeligt for en virksomhed at vide, om de eller deres produkt er omfattet af en konkret



¹ <http://data.europa.eu/eli/dir/2022/2555/2022-12-27>

² <http://data.europa.eu/eli/reg/2024/2847/oj>

³ Selvom alle detaljerne omkring henholdsvis NIS2-direktivet og Cyber Resilience Act endnu ikke er på plads, og der kan ske ændringer, er de overordnede rammer nogenlunde fastlagt.

lov, og hvordan kravene skal tolkes. Denne guide opridser love og krav, så virksomheden har mulighed for at afgøre om

- lovgivningen har relevans for dem, eller om de kan se bort fra den
- de måske er omfattet i et eller andet omfang, og de derfor bør følge udviklingen og se, hvordan de bliver berørt
- de tydeligt er omfattet af loven, og de derfor bør begynde at implementere de nødvendige tiltag allerede nu.

Guiden henvender sig primært til SMV'er, men kan også være et brugbart værktøj for større virksomheder, der har brug for hjælp til at få et overblik over den kommende EU-regulering inden for cybersikkerhed og få hjælp til at efterleve kravene. Ambitionen med guiden er at kunne hjælpe SMV'erne med at styrke deres cybersikkerhed, opretholde deres kunders tillid og styrke deres konkurrenceevne.

Udover at gennemgå Cyber Resilience Act og NIS2-direktivet indeholder guiden en generel introduktion til lovkrav på cyberområdet, hvor koblingen til standarder og CE-mærkning også berøres.

Præsentation af anvendte eksempler

For at konkretisere og gøre arbejdet mere håndgribeligt for SMV'er anvender guiden tre konkrete virksomhedseksempler. Eksemplene er fiktive men skitserer, hvordan typiske virksomheder/produkter kunne være berørt af lovgivningen, både direkte og indirekte. Virksomhederne i de tre eksempler har forskellige størrelser og modenhed, ikke kun med hensyn til cybersikkerhed i praksis, men også med hensyn til compliance og dokumentation. I den sammenhæng skal det nævnes, at et højt niveau af cybersikkerhed ikke nødvendigvis i praksis medfører et højt kompetenceniveau inden for compliance. Det samme gælder det modsatte; et højt niveau af compliance medfører ikke nødvendigvis et højt niveau af cybersikkerhed.

De tre virksomhedseksempler er udvalgt for at vise, hvordan kravene i henholdsvis NIS2-direktivet og Cyber Resilience Act påvirker forskellige typer af organisationer; herunder om de er direkte underlagt kravene, eller om kravene måske slet ikke er relevante for dem.





CASE A:

En mindre softwarevirksomhed med otte ansatte, hvis primære produkt er en app til smartphones. App'en bruges til energi-optimering af (primært) private hjem og integrerer med en husstands solceller, ladestander, varmepumper og andre el- og energiproducerende og -forbrugende apparater, man kan finde i en privat husstand. App'en er ikke kritisk, forstået på den måde, at alle apparater kan fungere uden den. App'en tillader, at husstanden kan forsøge at skrue op og ned på energiforbruget afhængigt af priser og andre (af brugeren) definerede parametre. Da virksomheden producerer software, har de ingen underleverandører af betydning. Virksomheden er ung og har ikke tidligere arbejdet med hverken cybersikkerhed eller compliance generelt. Der har ikke hidtil været et behov for dokumentation i forbindelse med produktet (software), og cybersikkerhed har virksomheden, ligesom den generelle IT-drift, klaret ad hoc.



CASE B:

En lille virksomhed med 35 medarbejdere, som producerer robotplæneklipper. Virksomhedens seneste linje af produkter anvender forskellige teknologier, bl.a. GPS og en cloudtjeneste, til at definere, hvilke plæneområder der skal klippes hvornår. Virksomheden har eksisteret i en årrække, og dens produkter er allerede omfattet af maskindirektivet og lavspændingsdirektivet. Virksomheden er derfor bekendt med compliancearbejde, og de har dokumentation udarbejdet i henhold til en række krav. Virksomheden har en enkelt IT-administrator ansat til at håndtere virksomhedens IT-drift og softwareudvikling, mens de øvrige ansatte primært har en baggrund inden for håndværk, fx smede og maskinmestre. De har derfor begrænset erfaring med IT, herunder cybersikkerhed. Virksomheden benytter en række underleverandører, som leverer de forskellige komponenter, fx motor, batteri og knive, der bliver samlet til en plæneklipper.



CASE C:

Et stort elselskab med ca. 1.200 ansatte, der leverer strøm til ca. 100.000 husstande. Uover elforsyning leverer selskabet også (fiber-)internet og installerer varmepumper samt ladestandere til elbiler. Virksomheden producerer ikke selv de varmepumper, ladestandere mv. de installerer, men benytter sig af produkter fra en række af andre virksomheder. Grundet virksomhedens størrelse er dens relationer til kunder og leverandører forholdsvis komplekse, idet nogle forhold er simple og generiske, mens andre relationer er unikke for leverandøren/kunden. Da virksomheden er inden for en reguleret sektor, laver virksomheden allerede et stort compliancearbejde, ligesom cybersikkerhed også er noget, virksomheden har arbejdet med i lang tid. I praksis betyder det, at virksomheden har dedikeret personale ansat til at sikre, at al relevant lovgivning er overholdt og dokumenteret, at der findes politikker for IT-sikkerhed, samt at der er tilstrækkelige ressourcer til at implementere sikkerhed i praksis. Virksomheden har implementeret en ledelsesstandard for informationssikkerhed, DS/EN ISO/IEC 27001, som de også er certificeret efter. Det betyder, at de allerede nu arbejder systematisk med processer for informationssikkerhed.

Introduktion til lovkrav på cyberområdet

Som nævnt i indledningen har EU store ambitioner på cybersikkerhedsområdet, hvilket betyder, at der igennem de seneste år er blevet introduceret en række initiativer og lovgivning på området, der skal bidrage til at sikre et mere sikkert digitalt EU. Den lovgivning, der kommer til at have den største indflydelse på danske virksomheder i forhold til implementering af krav om cybersikkerhed, er henholdsvis NIS2-direktivet og Cyber Resilience Act, som introduceres i det kommende afsnit.

Udover kravene i NIS2-direktivet og Cyber Resilience Act, som er omdrejningspunktet for denne guide, er der anden lovgivning, hvor

cybersikkerhed spiller en væsentlig rolle. Det gælder bl.a.

- radioudstyrsdirektivet, som nu også indeholder krav om cybersikkerhed til produkter med radioudstyr
- AI Act, som også stiller krav til cybersikkerheden i systemerne bag kunstig intelligens
- den kommende opdatering af maskinforordningen, som også kommer til at adressere cybersikkerhedskrav.

Korte beskrivelser af disse lovgivninger og kravene om cybersikkerhed kan ses i guidens annex.

Direktiv eller forordning?

En EU-lov kaldes for en retsakt. De mest almindelige former for retsakter kaldes forordninger og direktiver.

Forordninger er bindende retsakter, der gælder direkte i medlemslandene. Det betyder, at EU har besluttet, hvordan de danske domstole og myndigheder skal anvende forordningen.

Direktiver er retsakter, der fastlægger et fælles mål, der skal nås i alle EU's medlemslande. Det er op til de enkelte lande at bestemme, hvordan de vil gennemføre direktivet og opnå målet. Landene skal normalt gennemføre direktivet inden for to-tre år.

Når EU har vedtaget et direktiv, gælder det derfor først i Danmark, når Folketinget har implementeret det i dansk lovgivning. Derfor kan de nationale love, som er blevet indført på baggrund af direktivet, se forskellige ud fra medlemsland til medlemsland.

Modsat en forordning giver et direktiv derfor mere åbne rammer for, hvordan retsakten skal fortolkes og gennemføres i det enkelte medlemsland.

Kilde: Folketingets EU-oplysning

NIS2 er et direktiv og skal derfor implementeres i dansk lov med en dansk lovtekst. Cyber Resilience Act er en forordning og finder dermed direkte anvendelse i medlemslandene.



Koblingen mellem standarder og lovgivning

Når man taler lovgivning, giver det ofte mening også at forstå koblingen til standarder. Standarder er som udgangspunkt frivillige at anvende, mens det er et krav at følge gældende lovgivning. I nogle situationer kan standarder være tilknyttet direkte til lovgivning, hvilket er tilfældet med Cyber Resilience Act.



Man skelner mellem europæiske standarder og harmoniserede europæiske standarder. De harmoniserede standarder er bestilt af Europa-Kommissionen, og de relaterer sig direkte til lovgivning, hvilket er med til at sikre produkternes frie bevægelighed. Ved at følge de harmoniserede standarder har man som producent ret til at formode, at man

også opfylder lovgivningens væsentlige krav (formodningsret). Standarderne bliver med andre ord et hjælpemiddel for producenten til at dokumentere, at lovgivningens krav bliver opfyldt.

De europæiske standarder udvikles som udgangspunkt af de officielle europæiske standardiseringsorganisationer CEN, CENELEC og/eller ETSI, men kan i princippet også udvikles af Europa-Kommissionen selv. Under standardiseringsorganisationerne findes der en række tekniske komiteer, der udvikler standarder inden for afgrænsede fagområder, fx cybersikkerhed. I de tekniske komiteer er det eksperter fra hele Europa, der bidrager til udviklingen af de europæiske standarder. Eksperterne kommer fra små og store virksomheder, offentlige myndigheder, NGO'er, forbrugerorganisationer, uddannelses- og forskningsområdet, GTS-institutter osv.

Introduktion til CE-mærkning

De europæiske standarder spiller en helt central rolle for CE-mærkningen. Det gælder især de harmoniserede standarder, som er direkte koblet op på lovgivningen. På det digitale område har harmoniserede standarder indtil nu ikke været så udbredt, men i takt med udviklingen af den europæiske lovgivning på det digitale område følger også krav om harmoniserede standarder, bl.a. i forbindelse med både AI Act, radioudstyrsdirektivet og Cyber Resilience Act.

CE-mærket er producentens erklæring om, at et produkt lever op til den relevante lovgivning. CE-mærkning er ikke en certificering eller en godkendelse, men et mærke, der angiver, at man overholder visse krav til sikkerhed, sundhed og miljø inden for det pågældende produktområde. CE-mærket er et led i EU's ønske om at skabe fri bevægelighed af varer imellem EU-landene. Ved at stille ens krav til produkter gennem lovgivning, reducerer man tekniske handelshindringer, og

man sikrer, at de nationale myndigheder i et enkelt EU-land ikke kan stille strengere krav til et produkt end de krav, der er formuleret i loveteksten.

Som udgangspunkt er det producenten selv, der skal sørge for at CE-mærke produkterne. Når et færdigt produkt er klar til at blive markedsført, kan der dog være flere parter involveret, fx importører eller distributører. I forbindelse med CE-mærkning ligger det endelige ansvar hos den, der markedsfører produktet. CE-mærkning skal foretages af alle, der markedsfører et produkt i EU's medlemsstater og EFTA-landene Island, Liechtenstein, Schweiz og Norge, der er omfattet af EØS-aftalen. Når et produkt udelukkende fremstilles og markedsføres i Danmark, skal det også CE-mærkes.

De enkelte medlemslande i EU gennemfører en markedsovervågning for at beskytte forbrugere mod ikke-sikre produkter og forkert anvendelse af CE-mærkning. Det kontrolleres eksempelvis om

- produktet er CE-mærket
- produktet opfylder kravene
- mærket er udformet korrekt.

Hvis produktet ikke opfylder kravene, er der flere sanktionsmuligheder, fx indskærpeelse, politianmeldelse, bødeforlæg eller fjernelse af produktet fra markedet. Sanktionsmulighederne afhænger af, hvilken lovgivning produktet er underlagt.

For at sikre at kravene bliver overholdt, skal der udarbejdes en overensstemmelsesvurdering. For at gennemføre denne benyttes en defineret procedure, der kan være begrænset af den gældende lovgivning for produktet. Der er i alt otte metoder, der kan anvendes til CE-mærkning, hvoraf nogle har undervarianter. Disse er betegnet modul A-H og definerer producentens ansvar og krav om inddragelse af eventuel tredjepart. Den mest anvendte er modul A, som omfatter intern produktionskontrol, dvs. en

selv-evaluering. Et alternativ til denne er kombinationen af modul B og C, som er en tredjepartsgodkendelse. Hvis man vil gå i dybden med dette, kan det anbefales at læse Den blå vejledning om gennemførelse af EU's produktregler 2022⁴. På Dansk Standards hjemmeside⁵ kan man læse mere om CE-mærkning og få en guide til, hvordan et produkt CE-mærkes.

UKCA-mærket

Det nye UKCA-mærke (UK Conformity Assessment) er Storbritanniens produktmærke, der er en pendant til CE-mærket, men som kun gælder i Storbritannien. UKCA-mærket har været gældende fra januar 2021 for en række produkter, der markedsføres og sælges i Storbritannien (England, Wales og Skotland; Nordirland har UKNI-mærket). Mærkningen gælder for de fleste varer, der allerede er underlagt krav om CE-mærkning, samt en række øvrige kategorier.

Læs mere på den officielle britiske hjemmeside: <https://www.gov.uk/guidance/using-the-ukca-marking>

⁴ [https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52022XC0629\(04\)](https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52022XC0629(04))

⁵ <https://www.ds.dk/da/om-standarder/ce-maerkning>



Cyber Resilience Act

I efteråret 2024 vedtog Europa-Parlamentet og Rådet en ny forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer, Cyber Resilience Act (CRA). Forordningen er et led i den europæiske strategi for cybersikkerhed, og ambitionen er at styrke cybersikkerheden i produkter med digitale elementer, og dermed øge tilliden samt sikre retssikkerheden. Med forordningen følger fælleeuropæiske cybersikkerhedskrav for alle, der fremstiller, udvikler, importerer eller distribuerer produkter med digitale elementer, herunder både software og hardware.

Med den endelige vedtagelse i efteråret 2024 er der nu en 36 måneders indkøringsperiode for de tekniske krav og en 21 måneders indkøringsperiode for kravene, der er relateret til sårbarhedshåndtering.

Da der er tale om en forordning, skal den ikke implementeres nationalt, og den tilgængelige lovttekst har derfor også direkte virkning. De essentielle krav er allerede offentlige og kendte og skal være implementeret af producenter ultimo 2027.

Baggrund og formål

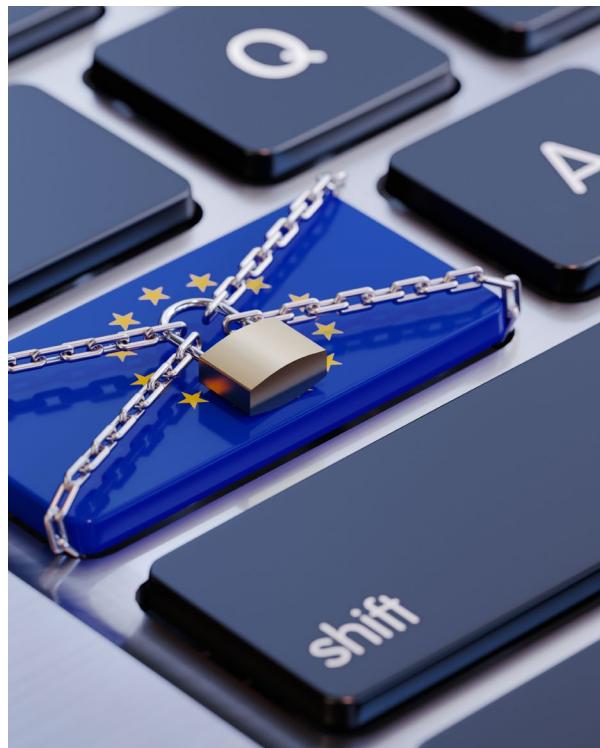
Formålet med Cyber Resilience Act er at sikre, at de digitale produkter, der kommer på markedet i EU, har et grundlæggende niveau af cybersikkerhed. Samtidig er det ambitionen at gøre det lettere for forbrugerne at gennemskue cybersikkerheden, når de vælger og bruger produkter med digitale elementer. Loven er bred og horisontal, hvilket betyder, at produkter som udgangspunkt er omfattet af loven, medmindre andre love stiller samme eller højere sikkerhedskrav.

Forordningen skelner mellem vigtige, kritiske og ikke-kritiske produkter, som har betydning for, hvordan man i praksis skal leve op til kravene (se figur 1). Der er defineret forskellige produkttyper, afhængig af produktets anvendelse, som er med til at bestemme, om et produkt anses som værende i kategorien

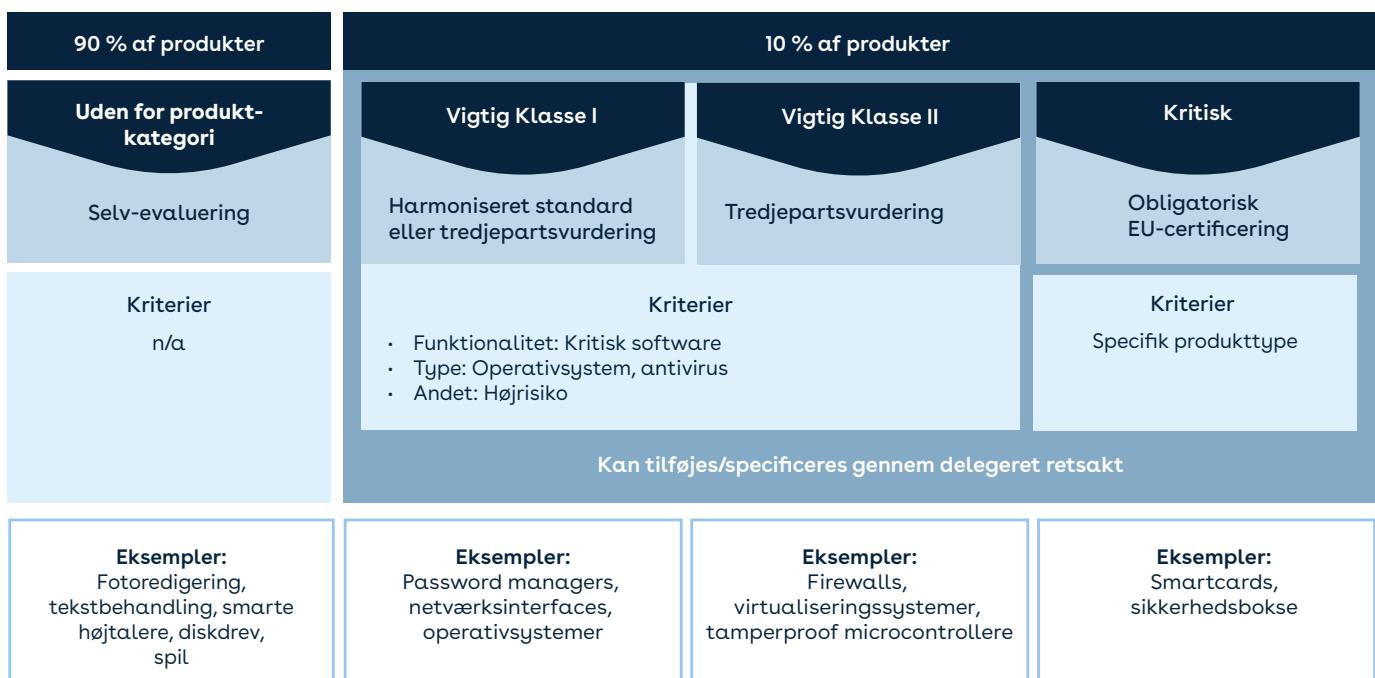
'vigtig'. Overordnet gælder det, at produktets primære funktion er at levere cybersikkerhedsfunktionaliteter, som er kritiske for andre produkter, eller hvor produktet bærer en væsentlig risiko for graden af skader, der kan ske i tilfælde af et brud. Vigtige produkter er desuden opdelt i to klasser. Hvilken kategori og klasse et produkt falder under, er bestemt af dets anvendelse.

For alle kategorier af produkter gælder de samme overordnede krav for, hvad produktet skal leve op til. Der, hvor der er forskelle, er i proceduren, der kan anvendes ved en overensstemmelsesvurdering. Fx kan der for ikke-kritiske produkter laves selv-deklarering (modul A), mens produkter i vigtig klasse II skal forbi et bemyndiget organ (modul B+C) for at få en tredjepartsgodkendelse.

Overtrædelse af reglerne i forordningen kan medføre betydelige bøder på op til 15 millioner euro eller 2,5 % af en virksomheds globale omsætning. Derudover kan producenter, hvis de ikke lever op til kravene, blive pålagt at fjerne eller tilbagekalde produkter fra markedet.



FIGUR 1. Produktklasser i Cyber Resilience Act



Hvad er kravene?

Selve loven opilater en række væsentlige krav, der er forholdsvis overordnet beskrevet. Kravene omfatter både tekniske krav og krav til virksomhedens processer.

Produkter skal udvikles således, at de har et passende niveau af sikkerhed afhængigt af en risikovurdering og den forventede brug af produktet. Med forordningen følger også krav om, at virksomheder skal rapportere eventuelle sikkerhedsbrud til EU's cybersikkerhedsmyndighed, ENISA, inden for 24 timer. Dette gælder i hele produktets levetid, og som konsekvens heraf skal producenterne offentliggøre produktets forventede levetid.

De mere tekniske krav indebærer bl.a., at et produkt ikke må indeholde kendte sårbarheder, når det sættes på markedet. Produktet skal beskyttes mod uautoriseret adgang, det skal designes, så konsekvensen ved et angreb minimeres, og der skal være mulighed for at sikkerhedsopdatere software/firmware.

Hvordan kravene præcist skal tolkes, vil blive nærmere beskrevet i en eller flere harmoniserede standarder. Disse standarder er under udvikling af eksperter fra hele Europa og skal være færdige i 2026.

Hjem gælder lovgivningen for?

Da forordningen dækker bredt, vil de kommende krav berøre både producenter, importører og distributører af hardware- og/eller softwareprodukter med digitale elementer. Producenterne har pligt til at sikre, at deres digitale produkter opfylder cybersikkerhedskrav og gennemgår overensstemmelsesvurderinger, før de sættes på markedet. Producenterne er også ansvarlige for cybersikkerheden gennem produktets livscyklus. Derudover skal de registrere teknisk dokumentation og overholde kravene til rapportering af cybersikkerhedsbrud. Importører må kun markedsføre produkter med digitale elementer, der opfylder de væsentlige cybersikkerhedskrav og er CE-mærket.

Distributører har ansvar for at sikre, at producenter og importører har overholdt deres forpligtelser i henhold til forordningen, og skal bekræfte, at de digitale produkter er CE-mærket.

Softwareprodukter er også omfattet af CRA. Software skal her forstås som programkode, der afvikles lokalt på et stykke hardware, hvorpå det er installeret. Dette betyder, dels at software skal gennemgå CE-mærkningsprocessen, og dels at det skal leve op til kravene under CRA. Man skal være opmærksom på, at selvom forordningen omfatter produkter, der "handles", betyder det ikke, at betaling nødvendigvis involverer penge. Det kan også være betaling med personlige data eller lignende. Der findes derudover særlige undtagelser/krav i forbindelse med open source-software.

Det er værd at understrege, at "fjern-databehandling" også er omfattet, dvs. hvis produktet (fx en smartphoneapp eller et netværksopkoblet kamera) er afhængigt af en cloudtjeneste eller lignende for at levere sin primære funktion. Samtidig skal det dog nævnes, at forordningen eksplisit nævner, at Software-as-a-Service (SaaS) ikke er omfattet, medmindre det er en del af et produkt med digitale elementer.

Forordningen dækker ikke produkter, som allerede er underlagt cybersikkerhedskrav i eksisterende sektorspecifikke EU-regler, fx medicinsk udstyr, luftfart og køretøjer. Forordningen dækker heller ikke produkter, der alene er udviklet til nationale sikkerhedsformål eller militære formål.

Koblingen til standarder

Europa-Kommisionen har bedt de officielle europæiske standardiseringsorganisationer (CEN, CENELEC og ETSI) om at udarbejde en række standarder, der skal hjælpe virksomhederne med at leve op til lovgivningen, ved at specificere, hvordan kravene overholdes. De standarder, der skal støtte op om den kommende lovgivning, vil blive udarbejdet fra 2024-2026 og skal dække de mere end 40+ krav, der er skrevet ind i forordningen. Nogle af de standarder, man forventer kommer til at gælde, findes allerede, men vil i forbindelse med standardiseringsanmodningen fra Europa-Kommisionen sandsynligvis blive justeret.

Selvom standarderne, der skal udspecifcere kravene under Cyber Resilience Act, er under udvikling, er der hjælp at hente i eksisterende standarder. Standarderne ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline requirements*⁶, DS/EN 18031-serien *Common security requirements for radio equipment* og DS/EN IEC 62443-4-2 *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components* indeholder en række tekniske krav i stil med de væsentlige krav, og man forventer, at de eksisterende standarder vil danne grundlaget for, hvordan (som minimum nogle af) kravene i CRA'en skal tolkes. Flere af de standarder, som kan hjælpe virksomheder, der arbejder med cybersikkerhed i produkter, er beskrevet i en guide udgivet af Dansk Standard⁷.

Udover de tekniske krav kan man også begynde at arbejde med de procesorienterede krav, dvs. man kan begynde at udarbejde processer for risikovurdering, processer for sikker udvikling samt processer for håndtering og indrapportering af sårbarheder.

⁶ Foruden ETSI EN 303 645 findes også ETSI TS 103 701 *Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements* og ETSI TR 103 621 *Guide to Cyber Security for Consumer Internet of Things*, der uddyber, hvordan kravene i ETSI EN 303 645 skal tolkes.

⁷ DS/PAS 2600:2021 *Cybersikkerhed i produkter (IoT)*: <https://www.ds.dk/da/download/ds-pas-2600-2021>

I den forbindelse kan det være relevant at orientere sig i standarderne DS/EN IEC 62443-4-1 *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*, DS/EN ISO/IEC 27005 *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*, DS/EN ISO/IEC 30111 *Information technology – Security techniques – Vulnerability handling processes* og DS/EN ISO/IEC 29147 *Information technology – Security techniques – Vulnerability disclosure*.

Det er vigtigt at understrege, at ovennævnte standarder kan bruges til at arbejde med de væsentlige krav, men de giver ikke formodningsret. Man forventer, at de kommende harmoniserede standarder vil trække på indholdet af de nævnte standarder, men det kan ikke udelukkes, at dele vil udgå, ligesom nye emner vil blive beskrevet i de harmoniserede standarder.

Hvilke krav skal SMV'erne forholde sig til?

Først og fremmest gælder det om at afgøre, om man udvikler produkter, der er omfattet af lovgivningen. Producerer man ikke produkter med digitale elementer, er loven ikke relevant.

Hvis man producerer omfattede produkter, skal man finde ud af, hvordan man skal gøre hele den efterfølgende proces an. Man vil sandsynligvis skulle arbejde i to spor:

- der skal implementeres en række sikkerhedstiltag
- der skal udarbejdes dokumentation for, hvordan sikkerhedstiltagene er implementeret.

De to spor hænger dog sammen, da kravene til, hvordan sikkerhedstiltagene skal dokumenteres, kan have indflydelse på, hvordan de implementeres. Hvis ens produkt er nævnt i forordningens bilag 3 eller 4, gælder der særlige regler

for, hvordan man skal dokumentere, at sikkerhedskravene er opfyldt, dvs. man skal anvende en harmoniseret standard eller forbi en tredjepart.

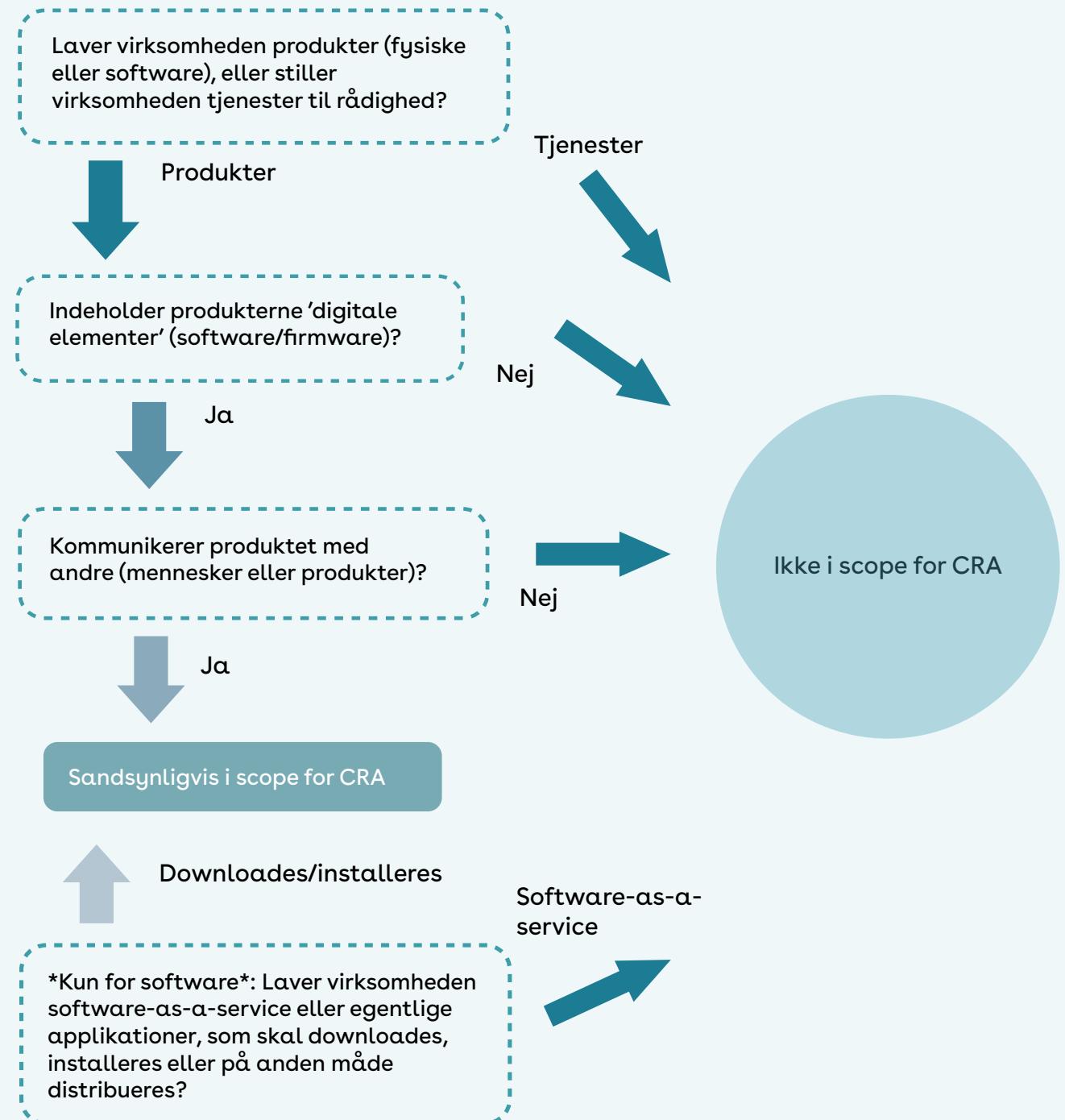
Hvis ens produkt ikke er nævnt i bilaget, er der bredere rammer for, hvordan man udfører sin overensstemmelsesvurdering. Man kan i principippet vælge selv at tolke de essentielle krav i bilag 1, men det kan være en fordel at læne sig op ad (dele af) eksisterende standarder. Her kan det desuden være en fordel at forhøre sig hos kunder og andre samarbejdspartnere, så man kommer til at arbejde med en standard, de anerkender.

Der vil som tidligere nævnt blive udarbejdet standarder specifikt tilpasset CRA, men disse ligger dog stadig et stykke ude i fremtiden. De kommende standarder vil dog (indholds-mæssigt) ligne de eksisterende standarder, så hvis man ønsker at påbegynde implementeringen, inden CRA-standarderne er klar, kan man eventuelt påbegynde den tekniske implementering med udgangspunkt i en anden standard (fx ETSI EN 303 645 eller DS/EN 18031-1) og vente med den formelle dokumentation, til CRA-standarderne er klar. Man undgår sandsynligvis ikke at skulle foretage nogle rettelser, når de endelige standarder ligger klar, men rettelserne burde blive forholdsvis små og forhåbentligt primært orienteret omkring dokumentation.

Da et af kravene er, at man sikrer produktet i hele dets levetid, bør man også begynde at overveje, hvad den forventede levetid af ens produkter egentlig er. Det vil formentlig blive en afvejning af kundernes ønsker/forventninger og ens egne forpligtelser.



FIGUR 2 – I scope for Cyber Resilience Act (CRA)?





CASE A:

Virksomhedens primære produkt er en smartphoneapp, og fordi denne både bliver solgt til forbrugere og kommunikerer via internettet, bliver den omfattet af Cyber Resilience Act. Det betyder, at virksomhed A fremover skal CE-mærke app'en og overholde de essentielle krav. Virksomheden har ikke tidligere arbejdet med compliance, og processen omkring CE-mækning er derfor ny for den.

Virksomheden vurderer selv, at produktet ikke fremgår af bilag 3 og 4, og de kan derfor i principippet selv vælge, hvordan de vil dokumentere, at de overholder kravene (modul A). Da mange af virksomhedens samarbejdspartnere er inden for energibranchen, er der et øget fokus på cybersikkerhed, og virksomheden ønsker derfor (eventuelt på sigt) at kunne dokumentere et højere sikkerhedsniveau, end det loven kræver.

Som resultat af ovenstående beslutter virksomhed A på kort sigt at tage udgangspunkt i DS/EN IEC 62443 (4-1 og 4-2) og kortlægge, hvordan disse dækker kravene i Cyber Resilience Act. Selvom standarderne er målrettet OT-systemer og ikke passer 100% på virksomhedens produkt, giver standarderne noget konkret at arbejde med på kort sigt, ligesom standarderne også bliver anerkendt af samarbejdspartnerne. På længere sigt følger virksomheden med i udviklingen af de harmoniserede standarder under Cyber Resilience Act, og når disse er udviklet, planlægger virksomheden at implementere de bedst egnede i forhold til deres anvendelsesområde. Den resulterende dokumentation bliver gemt internt. Udover den interne dokumentation udfylder virksomheden også den obligatoriske dokumentation (fx "EU Declaration of Conformity" fundet i bilag 5, 6 og 7 i Cyber Resilience Act). Selve "EU Declaration of Conformity" bliver sammen med CE-mærket, gjort tilgængelig på virksomhedens hjemmeside, ligesom selve CE-mærket bliver indsat i de relevante app-stores.

Virksomheden laver pt. kun den ene smartphoneapp, og ovenstående arbejde er orienteret omkring denne. Virksomheden er dog bekendt med, at hvis de i fremtiden laver et nyt, separat produkt, skal ovenstående gentages for dette. En række af de processer, som implementeres, er dog uafhængige af produktet og kan derfor genbruges i andre produkter.





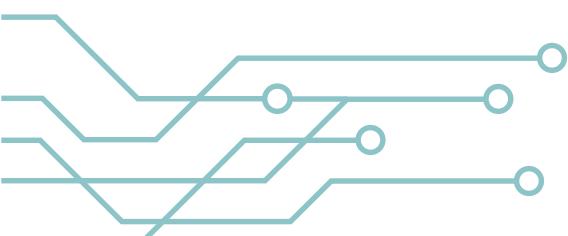
CASE B:

Ligesom virksomhed A producerer og sælger virksomhed B også et produkt, der kommunikerer over internettet, og derfor er virksomhed B's produkter også underlagt Cyber Resilience Act. Virksomhedens produkter er allerede CE-mærket i forbindelse med maskindirektivet, svagstrømsdirektivet og radioudstyrsdirektivet, og virksomheden har som konsekvens en ansat, som er inde i compliancereglerne. Virksomheden kan derfor hurtigt afgøre, at de ikke skal følge særlige krav, ligesom de vurderer, at deres kunder ikke stiller særlige krav i forbindelse med cybersikkerhed. Virksomheden vælger derfor at starte med at arbejde med de dele af ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline requirements*, hvor det giver mening. I praksis foregår det ved, at virksomheden gennemgår provisionerne i ETSI EN 303 645 og for hver enkel provision dokumenterer, hvordan deres produkt overholder provisionen (eller at den ikke er relevant). Ligesom virksomhed A følger virksomhed B med i udviklingen af harmoniserede standarder under Cyber Resilience Act, så virksomheden kan implementere en sådan, hvis dens anvendelsesområde er bedre egnet end ETSI EN 303 645.



CASE C:

Da virksomheden ikke selv producerer deres egne produkter, men derimod kun leverer en række tjenester, er virksomheden ikke underlagt Cyber Resilience Act. Skulle virksomheden blive bekendt med sikkerhedshuller i nogle af de fysiske produkter, de installerer ved kunden, giver Cyber Resilience Act dem mulighed for at inrapportere det til producenten af produktet.





NIS2-direktivet

Det nye net- og informationssikkerhedsdirektiv (NIS2) betyder, at alle EU's medlemslande bliver underlagt skærpede krav til cyber- og informationssikkerhed i forhold til kritisk infrastruktur. Kommissionen har udvidet anvendelsesområdet i forhold til det tidligere NIS-direktiv, som betyder, at endnu flere sektorer nu opfattes som kritisk infrastruktur. Derudover stiller direktivet implicit skærpede krav til de virksomheder, der leverer produkter og tjenester til kritisk infrastruktur. Det betyder også, at langt flere virksomheder vil skulle forholde sig til direktivet, for at finde ud af om og hvordan de er berørt af kravene.

Overordnet er kravene allerede kendte, og usikkerheden i lovgivningen handler primært om, hvorvidt den enkelte virksomhed kommer til at være omfattet. Kriterierne herfor er også kendte, men da det hele skal implementeres i national lovgivning, kan der opstå undtagelser og præciseringer i implementeringen. NIS2-direktivet forventes at blive implementeret i dansk lovgivning den 1. juli 2025.

Baggrund og formål

Det oprindelige NIS-direktiv blev vedtaget i 2016 og var den første fælles EU-lovgivning på cybersikkerhedsområdet. Direktivet blev vedtaget for at sikre et højt fælles sikkerhedsniveau for net- og informations-systemer i hele EU. Ifølge Europa-Kommissionen har det første NIS-direktiv ført til betydelige fremskridt i forhold til EU's samlede modstandsdygtighed over for cybertrusler. Men på baggrund af et stigende behov for en øget modstandsdygtighed i EU og et behov for et ensartet, højere niveau for cybersikkerhed på tværs af medlemslandene blev det foreslået at skærpe direktivet yderligere.

Det nye NIS2-direktiv medfører minimumskrav for cyber- og informationssikkerhed i hele EU for alle virksomheder og organisationer, som varetager kritiske og vigtige funktioner i samfundet. Ambitionen er at øge cybersikkerhedsniveauet i EU på længere sigt gennem en ensrettet implementering af kravene.

Direktivet sætter skærpert fokus på cybersikkerhed i forsyningskæder ud fra



erkendelsen af, at digitaliseringen har medført, at et cyberangreb ikke kun har konsekvenser for de direkte berørte, men påvirker hele forsyningsskæden. Og det kan potentielt resultere i vidtrækkende og langvarige negative konsekvenser på tværs af hele det indre marked.

Ambitionen med NIS2 er desuden at øge kravene til håndhævelse af reglerne og ensrette sanktionerne i hele EU. Derudover er der i det nye direktiv fokus på den ledelsesmæssige

forankring, hvilket konkret betyder, at ledelsen skal være bekendt med organisationens risikostyringsindsats. Derudover skal ledelsen også have godkendt de implementerede foranstaltninger samt have tilstrækkelige kompetencer til at forstå og vurdere cybersikkerhedsrisici.

Overblik over de nye krav fra NIS til NIS2

- **Flere virksomheder og organisationer er omfattet:** Private og offentlige enheder, der kvalificerer sig under definitionen mellemstore og store virksomheder, som leverer tjenester eller udfører aktiviteter i EU, er omfattet af NIS2. Mellemstore virksomheder er defineret ved et selskab, der har mellem 50-250 medarbejdere med en årlig omsætning på mellem 10 og 50 millioner euro (artikel 2). Da direktivet endnu ikke er blevet implementeret i dansk lovgivning, er det i øjeblikket uklart, hvilke virksomheder det præcist vil omfatte, herunder om det også inkluderer kommunerne.
- **Flere sektorer kategoriseres som kritisk infrastruktur:** I NIS2 bliver endnu flere sektorer betegnet som kritisk infrastruktur og er dermed underlagt de nye krav. De nye sektorer er bl.a. fødevareproduktion og affaldshåndtering.
- **Øget fokus på sikkerhed i forsyningsskæder:** Virksomheder omfattet af NIS2 pålægges at sikre, at deres leverandører også har et passende niveau af cybersikkerhed, således at den samlede forsyningsskæde er sikker.
- **Strengere tilsynsforanstaltninger:** De nationale myndigheder skal sørge for at føre tilsyn med de såkaldte væsentlige enheder.
- **Flere sanktionsmuligheder:** Hvis enheder eller sektorer ikke lever op til kravene om nødvendige foranstaltninger eller rapporteringspligt, har tilsynsmyndighederne sanktionsmuligheder i form af administrative bøder.
- **Underretningspligt på 24 timer:** Virksomheder og organisationer omfattet af NIS2 er underlagt en underretningspligt, som betyder, at hændelser med mistanke om brud på sikkerheden skal indrapporteres inden for 24 timer.
- **Større bøder:** Bødeniveauet hæves i forbindelse med overtrædelser af NIS2. Bøderne afhænger af en organisations type og størrelse.

Hvad er kravene?

Kravene til virksomheder består overordnet i, at virksomheden skal håndtere de risici, som cyberangreb udgør mod virksomheden selv og dennes kunder. Dette bliver nærmere specifiseret i 10 mere konkrete punkter i direktivets artikel 21, som bl.a. beskriver, at virksomheden skal udarbejde politikker for IT-sikkerhed, risikohåndtering, beredskabsplaner, træning ifm. IT-sikkerheden osv.

Mange af disse tiltag er allerede gængs praksis i forbindelse med IT-sikkerhed i mange virksomheder. Som noget nyt er der dog et særligt fokus på forsyningsskæder, dvs. hvordan underleverandører spiller ind i IT-sikkerheden, og at man har en pligt til at inrapportere, hvis man bliver utsat for en cyberhændelse⁸. Derudover er det også et eksplisit krav (artikel 20), at virksomhedens ledelse holdes ansvarlig for, at de ovenstående tiltag bliver implementeret.

Udover kravene til virksomhederne indeholder direktivet en række yderligere opgaver for medlemsstaterne. Der skal bl.a. udarbejdes en strategi for IT-sikkerhed, og der skal oprettes en række incidence response (CSIRT)-enheder, så indsatsen kan koordineres i tilfælde af cyberangreb.

De øgede krav til risikostyring har en central rolle i det nye NIS2-direktiv. Her præciseres det, at passende foranstaltninger som minimum indebærer, at virksomhederne udarbejder politikker for informationssikkerhed og risikoanalyse.

Minimumkravene for sikkerhedsforanstaltninger er udpegslet i direktivets artikel 21 og omfatter:

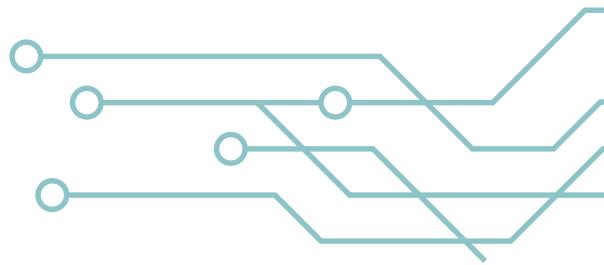
- politikker for risikoanalyse og informationssikkerhed
- håndtering af hændelser
- driftskontinuitet (back-up) og krisestyring
- forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører og tjenesteudbydere
- sikkerhed 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 tekstmunikation samt sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

⁸ Der findes allerede en lignende forpligtelse i GDPR, hvis persondata lækkedes.

Hvem gælder lovgivningen for?

De sektorer, der er omfattet af direktivet, bliver klassificeret på baggrund af deres betydning og opdelt i henholdsvis *væsentlige* og *vigtige enheder* (artikel 3). Kategorisering af virksomhederne påvirker, hvordan de bliver underlagt bl.a. sikkerhedskrav, sanktionering og tilsynsføring.

I NIS2-direktivets bilag 1 og 2 finder man en oversigt over sektorer af særligt kritisk betydning samt andre kritiske sektorer:



Sektorer af særligt kritisk betydning	Andre kritiske sektorer
<ul style="list-style-type: none">EnergiTransportBankvirksomhederFinansielle markedsinfrastrukturerSundhedDrikkevandSpildevandDigital infrastrukturForvaltning af IKT-tjenesterOffentlig forvaltningRummet	<ul style="list-style-type: none">Post- og kurertjenesterAffaldshåndteringFremstilling, produktion og distribution af kemikalierProduktion, tilvirkning og distribution af fødevarerFremstillingDigitale udbudereForskning

Som virksomhed eller organisation er det første skridt at finde ud af, hvorvidt man er omfattet af de nye krav i NIS2. Det bliver fastlagt endeligt i den danske implementering af direktivet, men for nogle virksomheder og sektorer står det allerede nu klart på baggrund af direktivets minimumskrav.

Som udgangspunkt gælder NIS2-direktivet ikke for mikrovirksomheder eller små virksomheder (mindre end 50 ansatte og omsætning mindre end 10 mio. euro), medmindre de har en høj sikkerhedsrisikoprofil, for eksempel hvis virksomheden har en særligt kritisk rolle i samfundet.

Koblingen til standarder

NIS2-direktivet opfordrer til at anvende internationale, anerkendte standarder (artikel 21 og 25). Men derudover er der ikke direkte krav om anvendelse af standarder.

DS/EN ISO/IEC 27001 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, som er en anerkendt, international ledelsesstandard for informationssikkerhed⁹, vil være en oplagt vej til at opfylde minimumkravene i NIS2-direktivet.

⁹ <https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed>

Standarden tilbyder en struktureret tilgang til at arbejde med informationssikkerhed, og en række af de minimumskrav, der er nævnt i NIS2, bliver konkretiseret med DS/EN ISO/IEC 27001 samt med standarden DS/EN ISO/IEC 27002 *Information security, cybersecurity and privacy protection – Information security controls*¹⁰, der indeholder en vejledning til kravene i DS/EN ISO/IEC 27001.

DS/EN ISO/IEC 27001 er en ledelsesstandard, der har fokus på den ledelsesmæssige forankring, hvorfor den også af den grund er et godt værktøj ift. NIS2, hvor der netop stilles krav til ledelsens ansvar.

Standarden er derfor et godt udgangspunkt for at arbejde med NIS2, da den netop behandler emner som hændelseshåndtering- og rapportering, politikker for informationssikkerhed og risikoanalyse samt praksisser for cyberhygiejne, som er en del af minimumskravene.

Alle virksomheder og organisationer uanset størrelse kan have glæde af at arbejde med DS/EN ISO/IEC 27001 og få skabt struktur på deres processer for informationssikkerhed. Standarden læses og implementeres i den kontekst, der giver mening for den enkelte organisation. Det er også muligt at blive certificeret efter DS/EN ISO/IEC 27001, men det er ikke et krav for at arbejde med standarden. Et af de væsentligste krav i NIS2 omhandler risikostyring, og netop af den årsag ser flere og flere virksomheder allerede i retning af ISO/IEC 27000-serien, da disse standarder har en risikobaseret tilgang. Standarderne er velførvede, internationale værktøjer, der kan hjælpe virksomhederne med at dokumentere deres risikostyringspraksis og hjælpe

med at identificere de passende foranstaltninger. Standarderne bidrager således til at rammesætte risikostyringsprocessen fra start til slut. Her kan standarden DS/EN ISO/IEC 27005 *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*¹¹ være en god hjælp, da den netop er en vejledning i risikostyring.

De mest relevante standarder i ISO/IEC 27000-serien ift. NIS2-arbejdet er følgende:

- DS/EN ISO/IEC 27001 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*
- DS/EN ISO/IEC 27002 *Information security, cybersecurity and privacy protection – Information security controls*
- DS/EN ISO/IEC 27005 *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*
- DS/ISO/IEC 27011 *Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations* (sektorspecifik)
- DS/ISO/IEC 27019 *Information security, cybersecurity and privacy protection – Information security controls for the energy utility industry* (sektorspecifik)

¹⁰ <https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed/iso-27002-foranstaltninger>

¹¹ <https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed/iso-27005-risikostyring>



Udover standarderne i ISO/IEC 27000-serien kan det også være oplagt at se nærmere på standarden DS/EN ISO 22301 *Security and resilience – Business continuity management systems – Requirements*. I NIS2 er der stort fokus på at sikre processer for forretningskontinuitet, sikkerhed i forsyningsskæden og beredskabsstyring, og her kan standarden være et godt sted at hente inspiration til det arbejde.

Hvilke krav skal SMV'erne forholde sig til?

Selve indholdet i direktivet er allerede vedtaget og offentliggjort. Usikkerheden vedrørende lovgivningen omhandler derfor primært, hvorvidt virksomheden er omfattet, og hvordan man dokumenterer tilstrækkeligt, at man opfylder kravene. Hvis man ikke er helt sikker på, hvorvidt man er omfattet af lovgivningen, giver det mening at se på, hvordan man arbejder med IT-sikkerhed, og om der er plads til forbedringer.

Hvis man allerede har et ledelsessystem for informationssikkerhed (ISMS), fx baseret på DS/EN ISO/IEC 27001, opfylder man sandsynligvis de fleste af direktivets krav, og det bliver dermed primært et spørgsmål om at dokumentere sin praksis. I den forbindelse kan man gennemgå sit ISMS, måske med et særligt fokus på, hvordan leverandører håndteres, og se om kravene er adresseret. Man kan også undersøge sine processer i forbindelse med beredskabsplaner og hændelseshåndtering, så man sikrer, at man kan leve op til kravene om at kunne inrapportere hændelser inden for tidsfristen. Når kravene i den nationale implementering derefter bliver offentligt tilgængelige, kan man arbejde videre med dokumentationskravene.

Hvis man ikke tidligere har arbejdet med cyber- og informationssikkerhed på et strategisk niveau, kan man begynde med at se på DS/EN ISO/IEC 27001 og DS/EN ISO/IEC 27002. Man behøver ikke at lave en fuld implementering, men standarderne kan bruges som inspirationskatalog for tiltag, man kan/bør implementere. Risikostyring er

eksplicit nævnt i direktivet, så det bør man også begynde at kigge nærmere på, uanset om man vælger DS/EN ISO/IEC 27001-tilgangen eller noget andet. Hvis man aldrig har arbejdet med risikostyring, kan man få en kort introduktion i Dansk Standards guide til risikostyring¹².

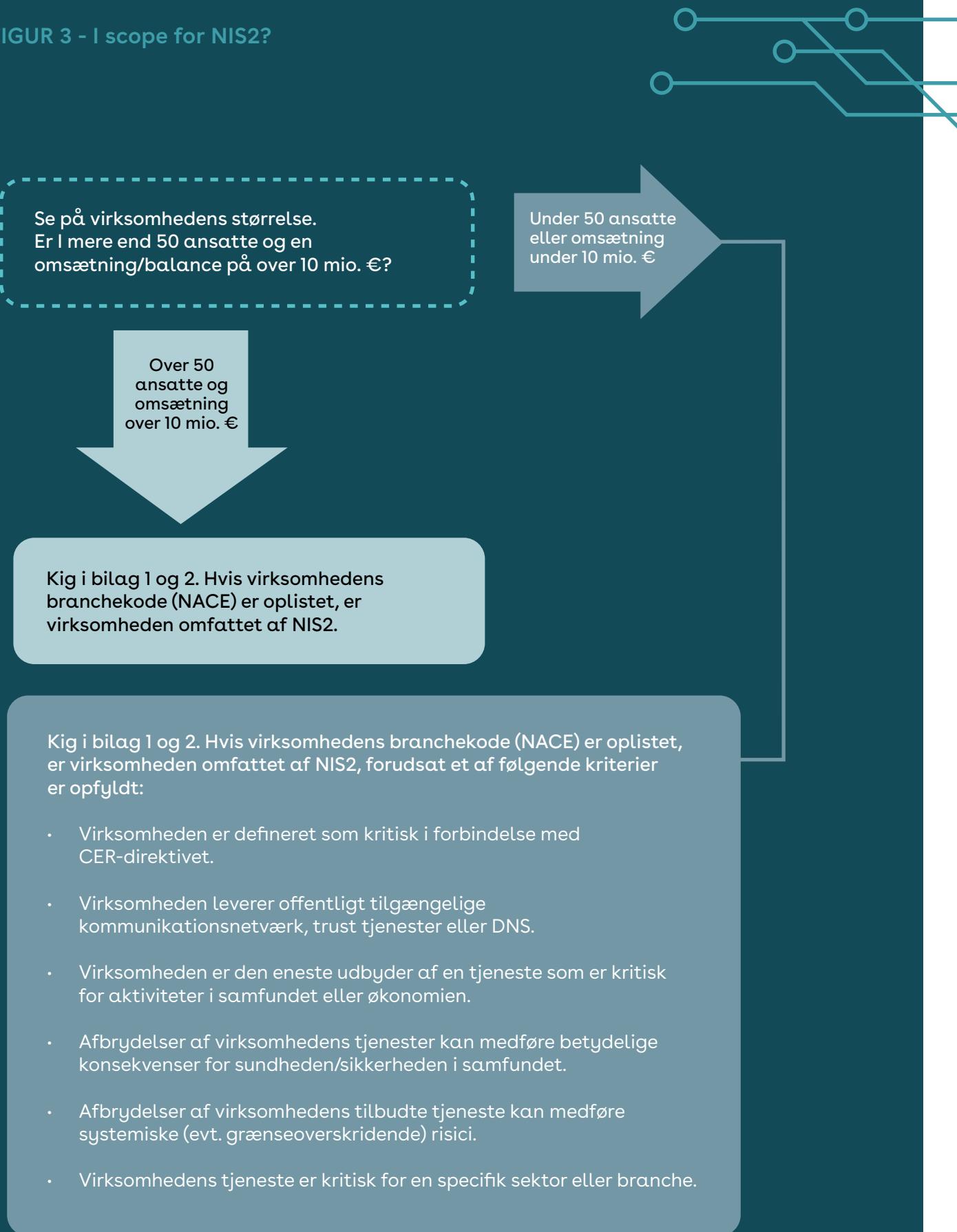
For (mindre) danske virksomheder kan det også give mening at kigge i retningen af D-mærket. D-mærket kan ses som en mere simpel tilgang for SMV'er end DS/EN ISO/IEC 27001 og DS/EN ISO/IEC 27002. D-mærket er dog ikke lige så detaljeret som standarderne og kan ikke tilpasses i samme grad. Hvor DS/EN ISO/IEC 27001 sandsynligvis opfylde alle kravene i direktivet, er der ikke helt samme sandsynlighed omkring D-mærket. En mulig tilgang kan derfor være at starte med at arbejde med D-mærket og derefter, når man opfylder kravene her, arbejde videre med DS/EN ISO/IEC 27001.

Det giver også mening at starte en dialog med sine leverandører om, hvordan de arbejder med cybersikkerhed.

NIS2 specificerer ikke, hvilke krav der skal stilles til leverandøren, og det er derfor tilladt at stille varierende krav afhængigt af leverandørens kritikalitet. Kravene og standarderne beskrevet i afsnittet om CRA kunne være udgangspunktet mht. sikkerhed i produkter, mens DS/EN ISO/IEC 27001 og D-mærket kunne være en mulighed mht. leverandørens drift.

¹² <https://www.ds.dk/da/om-standarder/viden/cyber-og-informationssikkerhedsstandarder/guide-til-riksikostyring>

FIGUR 3 - I scope for NIS2?





CASE A:

Da virksomheden er forholdsvis lille og ikke er inden for en branche, der er beskrevet i direktivet, er virksomheden ikke underlagt kravene i NIS2. Virksomheden har dog en række samarbejdspartnere, som er omfattet, og virksomhed A er bekymret for, hvordan disse vil begynde at stille krav til dem.

Der er altså ingen formelle krav til virksomheden, men ved at følge en relevant standard forventer virksomhed A, at det vil blive lettere at kommunikere med samarbejdspartnere. På baggrund af dette vælger virksomheden at bruge D-mærket til en hurtig gap-analyse, så der kan sættes ind, hvis der viser sig at være større mangler. Virksomheden begynder derefter proaktivt at forhøre sig hos samarbejdspartnerne om, hvilke krav de stiller til virksomheden, og hvorvidt D-mærket er tilstrækkeligt.



CASE C:

Virksomhed C er uden tvivl omfattet af loven, da den både er en stor mht. ansatte og arbejder inden for kritisk infrastruktur. Grundet disse omstændigheder har virksomheden dog allerede et højt modenhedsniveau mht. sikkerhed, eksempelvis er virksomheden allerede ISO/IEC 27001-certificeret.

Da virksomheden allerede har en lang række sikkerhedstiltag implementeret og et ledelsessystem for informationssikkerhed, formoder virksomheden, at det primært er småting, der skal arbejdes med for at være compliant. Direktionen nedsætter en arbejdsgruppe bestående af repræsentanter fra både teknikere og ledelsen, der referer til bestyrelsen. Arbejdsgruppen udarbejder først en gap-analyse i forhold til lovteksten, så de kan begynde at arbejde med eventuelle huller. Arbejdsgruppen følger samtidig med i den danske udvikling inden for loven, så der kan tages hensyn til eventuelle danske tolkninger af loven.



CASE B:

Modsat virksomhed A optræder virksomhed B's branchekode i bilaget i NIS2-direktivet. Virksomheden har dog under 50 ansatte og er derfor ikke omfattet. Da virksomheden ikke formelt er omfattet og ikke forventer at blive mødt af særlige krav fra kunder og leverandører, starter virksomheden ikke nye tiltag. Direktivet kommer dog på direktionens dagsorden med passende intervaller, så det løbende kan vurderes, om der skal gøres nye tiltag.

Opsamling

De kommende lovkrav i henholdsvis NIS2-direktivet og Cyber Resilience Act kan for flere virksomheder betyde, at der er behov for at udarbejde eller videreudvikle en strategi for cybersikkerhed, der forholder sig til indholdet. For mange kan det virke som en uoverskuelig proces, men sådan behøver det ikke at være. Første skridt vil være at vurdere, om man er omfattet, og i hvilken grad. Hvis man er omfattet, vil næste skridt være at vurdere, om og i hvilken grad man allerede arbejder med de krav, som direktivet eller forordningen stiller, og hvor der er behov for at fokusere arbejdet.

Arbejdet med de kommende cybersikkerhedskrav skal ikke kun ses som en compliance-øvelse. Der er bestemt mange fordele ved at arbejde mere systematisk med cyber- og informationssikkerhed. Først og fremmest er det værdifuldt at få etableret interne processer i organisationen, der gør det tydeligt for alle, hvilke krav der skal leves op til, og hvem der gør hvad. Eksternt er der bestemt også fordele ved at have udarbejdet en

cybersikkerhedsstrategi og have styr på, hvilke krav man skal leve op til. På sigt kan det potentielt skabe nye forretningsmuligheder ift. samarbejdspartnere og leverandører, da de kan se en fordel i at samarbejde med en virksomhed, der har styr på deres arbejde med cyber- og informationssikkerhed.

Til trods for at vi ikke kender de endelige lovkrav endnu, er det en god idé allerede nu at starte arbejdet op. Som det er nævnt ovenstående, er der allerede mange steder at hente hjælp til sit arbejde med bl.a. risikostyring, sårbarhedshåndtering osv. Standarderne er internationale, anerkendte og udbredte, og de kan anvendes som redskabskasse for virksomhedens arbejde med en cybersikkerhedsstrategi.

God arbejdslyst!

Anneks

AI Act (AI-forordningen)¹³

AI Act er den første europæiske lovgivning om brugen og udviklingen af kunstig intelligens. Lovgivningen trådte i kraft i august 2024.

AI Act er en forordning, der kategoriserer kunstig intelligens efter fire risikoniveauer, som er retningsgivende for, hvilke forpligtelser udbydere og brugere af kunstig intelligens skal leve op til. Dvs. jo højere risikoneveau, desto flere krav og forpligtelser.

De fire risikoniveauer er:

- uacceptabel risiko (forbudt)
- højrisiko (overensstemmelsesvurdering)
- begrænset risiko (gennemsigtighed)
- minimale risici (adfærdskodeks).

AI Act stiller også krav til cybersikkerheden i AI-systemer, og kravene vil blive suppleret med standarder, der hjælper virksomhederne med at leve op til lovkravene, på samme måde som med Cyber Resilience Act.

¹³ <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Radio Equipment Directive (RED) – Delegated Acts (Radioudstyrsdirektivet – delegerede retsakter)¹⁴

I 2021 besluttede Europa-Kommissionen at aktivere de delegerede retsakter i radioudstyrsdirektivet (artikel 3, stk. 3, litra d) e) og f)), der omhandler cybersikkerheden i produkter med radioudstyr. De nye krav gælder for alt radioudstyr, der selv kan kommunikere via internettet, uanset om det kommunikerer direkte eller via et andet udstyr. Lovgivningen finder anvendelse fra 1. august 2025, hvilket betyder, at alle produkter, der kommer på markedet herefter, skal leve op til lovprisen.

Samtidig med at de delegerede retsakter blev aktiveret, bad Europa-Kommissionen de officielle europæiske standardiseringsorganisationer om at udarbejde standarder med henblik på at hjælpe europæiske virksomheder med at overholde lovprisen. Ambitionen har været at kunne harmonisere standarderne, så virksomhederne, der anvender dem, har formodningsret, dvs. at man ved at følge standarderne efterlever kravene i direktivet.

- DS/EN 18031-1 *Common security requirements for radio equipment – Part 1: Internet connected radio equipment*
- DS/EN 18031-2 *Common security requirements for radio equipment – Part 2: Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment*
- DS/EN 18031-3 *Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value*

De tre standarder blev udgivet i august 2024 og afventer ved guidens udgivelse afklaring ift. harmonisering. (det skal vi have skrevet om, hvis der kommer afklaring inden deadline)

De tre standarder forventes at spille ind i de kommende standarder, der skal udvikles under Cyber Resilience Act.

¹⁴ https://eur-lex.europa.eu/eli/reg_del/2022/30/2023-10-27

Revised Product Liability Directive (Direktivet om produktansvar)¹⁵

Direktivet har eksisteret i mange år og skal grundlæggende sikre, at producenter kan holdes ansvarlige, hvis deres produkt er defekt og derved skyld i en skade ved kunden.

For at modernisere direktivet bliver der eksplisit gjort opmærksom på, at software (i bred forstand) skal betegnes som et produkt, både hvis det er "stand-alone", og hvis det indgår i en anden komponent, fx en smartphoneapp eller styringen i en varmepumpe. Ligeledes har direktivet tidligere haft et fokus på fysisk skade, hvilket fremover ændres, så immateriel skade, dvs. "datatab", også er omfattet. Endelig vil manglende cybersikkerhed i et produkt juridisk set blive betegnet som en defekt.

Ændringerne vil samlet set betyde, at hvis et produkt (inkl. software) bliver hacket på grund af manglende sikkerhed, vil man som producent/udvikler kunne holdes ansvarlig.

Selve direktivet indeholder ikke tekniske krav, man skal overholde, men nævner, at ved at følge relevante krav, eksempelvis fra CRA, vil man kunne reducere et evt. ansvar, man måtte have. Det betyder, at hvis man generelt implementerer et rimeligt niveau af cybersikkerhed, burde loven ikke være en udfordring.

General Product Safety Regulation (GPSR) (Forordningen om produktsikkerhed i almindelighed)¹⁶

EU's forordning om produktsikkerhed har til formål at sikre forbrugernes sundhed og sikkerhed generelt og har ikke direkte fokus på cybersikkerhed. Forordningen dikanterer, at kun "sikre produkter" må bringes på markedet i EU. Når produktets art kræver det, fx hvis påvirkning udefra kan påvirke sikkerheden, skal produktets egenskaber mht. cybersikkerhed indgå i vurderingen af, om produktet er sikkert. Hvis produktet anvender AI, skal der ligeledes tages hensyn til, hvad produktet kan lære i sin levetid, og hvorvidt det gør produktet usikkert.

Machinery regulation (Forordningen om maskiner)¹⁷

Maskiner har hidtil været reguleret under maskindirektivet, som nu laves om til en forordning. Forordningen skal anvendes fra 2027 og indeholder en række krav, der skal sikre, at maskiner ikke er "farligt". I den nye forordning er cybersikkerhed også noget, der skal sikres, så et cyberangreb ikke kan forårsage en farlig situation. Man skal fx sikre, at maskinen ikke spontant tænder, at en evt. sluk-knap ikke kan deaktivieres osv.

¹⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>

¹⁶ <https://eur-lex.europa.eu/eli/reg/2023/988/oj>

¹⁷ <https://eur-lex.europa.eu/eli/reg/2023/1230/2023-06-29>

Cyber Security Act (CSA) (Forordningen om cybersikkerhed)¹⁸

Den europæiske forordning om cybersikkerhed trådte i kraft i 2021. Forordningen indeholder ikke direkte krav til virksomheder eller borgere i EU. Loven har to funktioner: For det første opstiller den rammerne for ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), der, indtil Cyber Security Act blev vedtaget, kun var finansieret på projektbasis. For det andet etablerer forordningen en fælles europæisk cybersikkerhedscertificeringsramme for IKT-produkter, -tjenester og -processer. Cybersikkerhedscertificeringen er som udgangspunkt frivillig og skal bidrage til at dokumentere, at IKT-produkter, -tjenester og -processer opfylder specifikke krav. Produkterne eller tjenesterne certificeres efter forskellige kriterier og tildeles et 'grundlæggende', 'betydeligt' eller 'højt' sikkerhedsniveau. Sikkerhedsniveauerne anvendes til at informere brugerne om cybersikkerhedsrisikoen ved et produkt. Et højt sikkerhedsniveau betyder, at det certificerede produkt består de højeste sikkerhedstests. I første omgang udarbejdes der tre certificeringsordninger for cybersikkerhed: EUCC (European Common Criteria), EU Cloud og EU 5G. De virksomheder, der gennemgår certificering, opnår et cybersikkerheds-certifikat (overensstemmelsesattest), der beviser, at de opfylder kravene i en relevant certificeringsordning for cybersikkerhed. Certificeringerne garanterer ikke, at produktet, processen eller tjenesten har et passende sikkerhedsniveau, men blot at sikkerheden er evalueret på et vist niveau. Certifikaterne udstedes af en uafhængig certificeringsinstans og anerkendes i alle EU-medlemsstater.

Cyber Solidarity Act (Forordningen om cybersolidaritet)¹⁹

Cyber Solidarity Act har til formål at styrke samarbejdet omkring cybersikkerhed i EU. Loven danner bl.a. grundlag for et øget samarbejde omkring opdagelse af og varsling af (større) cyberangreb på EU-medlemsstater. Loven skaber også grundlag for et beredskab af sikkerhedsekspertir, der kan hjælpe, hvis en medlemsstat bliver utsat for større cyberangreb.

¹⁸ <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

¹⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209>

Bibliografi

Standarder og øvrige publikationer udgivet af Dansk Standard er dynamiske og bliver løbende evalueret og revideret, ligesom der kan blive udgivet rettelsesblade og tillæg til den enkelte standard/publikation. Alle standarder/publikationer var gældende på udgivelsestidspunktet for denne guide, men følg altid status i Dansk Standards webshop, www.webshop.ds.dk, hvor de også kan købes.

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive: https://eur-lex.europa.eu/eli/reg_del/2022/30/2023-10-27

Den blå vejledning om gennemførelse af EU's produktregler 2022:

[https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52022XC0629\(04\)](https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52022XC0629(04))

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive): <http://data.europa.eu/eli/dir/2022/2555/2022-12-27>

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC:

<http://data.europa.eu/eli/dir/2022/2557/oj>

DS/PAS 2600 Cybersikkerhed i produkter (IoT):

<https://www.ds.dk/da/download/ds-pas-2600-2021>

DS/EN 18031-1 Common security requirements for radio equipment – Part 1: Internet connected radio equipment

DS/EN 18031-2 Common security requirements for radio equipment – Part 2: Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

DS/EN 18031-3 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline requirements

ETSI TR 103 621 Guide to Cyber Security for Consumer Internet of Things

ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements Folketingets EU-oplysning: <https://www.eu.dk/>

Guidance using the UKCA marking: <https://www.gov.uk/guidance/using-the-ukca-marking>

Guide til risikostyring – risikostyring i forhold til cyber- og informationssikkerhed for SMV'er: <https://www.ds.dk/da/om-standarder/viden/cyber-og-informationssikkerhedsstandarder/guide-til-risikostyring>

Hvad er CE-mærkning?: <https://www.ds.dk/da/om-standarder/ce-maerkning>

DS/EN IEC 62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

DS/EN IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

DS/EN ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements

DS/EN ISO/IEC 27002 Information security, cybersecurity and privacy protection – Information security controls

DS/EN ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks

DS/ISO/IEC 27011 Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations

DS/ISO/IEC 27019 Information security, cybersecurity and privacy protection – Information security controls for the energy utility industry

DS/EN ISO/IEC 29147 Information technology – Security techniques – Vulnerability disclosure

DS/EN ISO/IEC 30111 Information technology – Security techniques – Vulnerability handling processes

Proposal for a directive of the European Parliament and of the Council on liability for defective products: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>

Proposal for a regulation of the European Parliament and the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209>

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act): <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC: <https://eur-lex.europa.eu/eli/reg/2023/988/oj>

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC: <https://eur-lex.europa.eu/eli/reg/2023/1230/2023-06-29>

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance): <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act): <http://data.europa.eu/eli/reg/2024/2847/oj>

