Forslaget til NIS 2-loven

Cybersikkerhed og juridisk compliance i praksis

Christian Wiese Svanberg
Partner, CO:PLAY Advokatfirma

E-mail: cws@coplay.law
Telefon: +45 2275 2646

CO:PLAY

Christian Wiese Svanberg

Erfaring (uddrag)

- Datatilsynet
- Justitsministeriet

Sad bl.a. med forhandlingen af GDPR under Danmarks EU-formandskab

- Advokat hos Plesner

Speciale i databeskyttelse

- Rigspolitiet

Databeskyttelsesrådgiver og chef for Center for Databeskyttelse

- Forsvarets Efterretningstjeneste/CFCS

Juridisk afdelingschef med ansvar for bl.a. signal indhentning (SIGINT), offensiv cyber (CNE/CNO) og cybersikkerhed (CFCS), herunder implementering af NIS 2

Agenda

I. Kort om status på lovgivningsprocessen, hvem er omfattet mv.
II. Klare svar på svære spørgsmål?: Er de kommende regler nu præciseret nok til, at man kan gå i gang?

Temaer:

I. § 6-kravene
II. Leverandørstyring
III. Håndtering af hændelser

III. Spørgsmål

Take-aways ”up front”

- Cybersikkerhed er nu såvel en retlig, som en praktisk disciplin.
- Compliancearbejdet skal gå på ”to ben”, for at styre jeres relevante risici: Det cybersikkerhedsfaglige og det juridiske. Ideelt set skal de forenes og gå takt.
- Det handler faktisk ikke om cybersikkerhed…
- Alle dele af arbejdet kan styres og gøres håndterbare ved at holde fokus på, hvorfor reglerne indføres.
- Det er én af den slags opgaver, der bedst løses ved at gå i gang (uddybning følger).

Status på lovgivningsprocessen

Kort status på lovgivningsprocessen

- Høringsfristen er 22. august 2024
- Parallel behandling af lovforslag om gennemførsel af CER-direktivet (kritiske enheders modstandsdygtighed)
- Lovforslaget fremsættes nok i oktober og vedtages inden nytår.
- Loven vil træde i kraft 1. marts 2025.
- Der må forventes omfattende opmærksomhed og høringssvar, men jeg er skeptisk ift., hvor meget mere konkret lovforslaget samlet set vil ende med at være, når det fremsættes.


Hvem er omfattet?

CO:PLAY

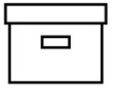
Væsentlige enheder

Essential entities


Digital infrastruktur


Energi


Transport


Offentlig forvaltning


Bank- & finansiel markedsinfrastruktur


Sundhed


Drikke- og spildevand

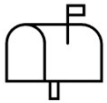

Rummet

Vigtige enheder

Important entities


Kemikalier


Affaldshåndtering


Post- og kurervirksomhed


Fødevarevirksomheder


Digitale serviceudbydere


Forskning


Produktionsvirksomheder af særlig vigtigt udstyr

Minimumskrav

NIS 2-loven gælder kun for mellemstore virksomheder, der lever op til en eller flere af følgende krav, og er en væsentlig eller vigtig enhed:

+50 medarbejdere i virksomheden

+75 mio. kr. i omsætning (+10 mio EUR)

+75 mio. kr. i formueopgørelse (+10 mio. EUR)

Hvem er omfattet?

- De omfattede sektorer (forrige slide) omfatter også hele staten.
- Kommuner er ikke omfattet som sektor, men der er adgang for at digitaliseringsministeren ved bekendtgørelse kan fastsætte, at kommuner bliver omfattet.

  ”Det er på nuværende tidspunkt ikke intentionen at fastsætte regler om, at kommunerne og lokale folkekirkelige myndigheder omfattes af loven.” (lovforslagets bemærkninger)
- Samtidig vil kommuner, der udøver aktiviteter i en omfattet sektor, være omfattet i forhold til disse aktiviteter.

Hvem er omfattet?

- ”I det omfang kommuner eller regioner måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og er af en størrelse, der svarer til tærsklerne for mellemstore virksomheder, anses de for at være væsentlige enheder.”

Hvor dyrt bliver det?

Virksomheder:

”De erhvervsøkonomiske konsekvenser ved gennemførelsen af NIS 2-di-rektivet i dansk ret (er) foreløbigt estimeres i et spænd på ca. 2,6 mia. kr. til 3 mia. kr. i omstillingsomkostninger”

”en gennemsnitlig virksomhed skal bruge 22-25% af sine nuværende omkostninger til it-sikkerhed på at omstille sig til kravene i NIS 2-direktivet. Tallet er 12-15% for virksomheder, der allerede er omfattet af NIS 1-direktivet. Europa-Kommissionens konsekvensvurdering indeholder ikke en kvantificering af de løbende omkostninger.”

”…danske virksomheder(som median) har omkostninger til it-sikkerhed på 825.000 euro pr. virksomhed.”

Hvor dyrt bliver det?

Det offentlige:

”De statsfinansielle konsekvenser til øgede aktiviteter afstedkommet af lovforslaget estimeres med betydelig usikkerhed at udgøre ca. 105-147 mio. kr. årligt.
Derudover estimeres der med betydelig usikkerhed at være udgifter i regionerne på 63-100 mio. kr. årligt.
Der estimeres endvidere med betydelig usikkerhed at være udgifter i kommunerne på 95-280 mio. kr. årligt. Der vurderes desuden at være negative implementeringskonsekvenser.”

(lovforslagets generelle bemærkninger)


Klare svar på svære spørgsmål?

Ét klart svar

”Det afgørende element for, hvilke af enhedens net- og informations-systemer, der er underlagt direktivets krav, bliver på den baggrund, hvorvidt der ud fra en konkret risikovurdering er tale om net- og informationssystemer, som – hvis de blev kompromitteret – vurderes at ville kunne påvirke enhedens levering af de tjenester eller opretholdelse af de aktiviteter, som er baggrunden for, at enheden er omfattet af direktivet.”

Lovforslagets bemærkninger punkt 3.1.2.

Dagens triste ”nyhed”

Kommuner oplever rekordmange hackerangreb:
Men ansvaret ligger hos dem selv, siger minister

IT-sikkerhed | 19. august kl. 09:58 | 1

Illustration: Digitaliserings- og ligestillingsministeriet.

Det er kommunernes eget ansvar at prioritere cybersikkerheden, lyder det fra digitaliseringsminister Marie Bjerre (V) oven på flere hackerforsøg mod fynske kommuner.

Lasse Skovgaard

Følg +

Et flertal af de fynske kommuner har i løbet af de seneste tre år oplevet en stigning i antallet af forsøg på hackerrangreb, skriver TV 2 Fyn på baggrund af en rundspørge.

16. AUG 2024, 07:29

Minister ser alvorligt på kampen mod hackere

Af **Anders Bøttcher**

Cybertruslen på Fyn er større end aldrig før.

Et flertal af de fynske kommuner har oplevet en stigning i antallet af forsøg på cyberangreb gennem de sidste tre år. Det viser en rundspørge, som TV 2 Fyn har lavet.

Det er en alvorlig stigning, mener Digitaliserings- og Ligestillingsminister Marie Bjerre.

- Vi kan se, at der er en større trussel og dermed også et større behov for at være mere sikker. Derfor er det godt, at kommunerne er opmærksomme på det.

Flere af kommunerne, TV 2 Fyn har talt med, efterlyser hjælp fra staten til at bekæmpe cyberangreb. Det er dog ikke så simpel en opgave.

- Ansvaret bliver nødt til at være hos kommunerne, når vi i Danmark har kommunalt selvstyre. Det er dem selv, der køber udstyret, og det er dem, der har dataen. Det giver ikke mening at adskille det. Derfor har de selv ansvaret for at prioritere cybersikkerheden, og det er vigtigt at prioritere, siger Marie Bjerre.

Selvom kommunerne står på egne ben, anerkender staten, at der er behov for en økonomisk oprustning på cyberområdet.

- Det er noget, vi bliver nødt til at tage alvorligt. Heldigvis lavede vi med den seneste økonomiaftale et gevaldigt løft til kommunerne. Fra næste år bliver der stillet yderligere krav til cybersikkerheden, og der bliver indført tilsyn på området. Ud fra de krav vil vi kunne se og drøfte med kommunerne, om der er behov for yderligere økonomiske ressourcer, siger Marie Bjerre.

FACEBOOK TWITTER KOPIÉR LINK

§ 6-kravene

- **§ 6.** Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte eller tage højde for:

- 1) Politikker for risikoanalyse og informationssystemsikkerhed.
- 2) Håndtering af hændelser.
- 3) Driftskontinuitet, eksempelvis backup-styring og reetablering efter en katastrofe, og krisestyring.
- 4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.
- 5) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.
- 6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.
- 7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.
- 8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.
- 9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
- **10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.**

Sektorspecifikke bekendtgørelser

- Forsvarsministeren og den relevant ressortminister, vil udstede ”sektorspecifikke bekendtgørelser”, der præciserer kravene i § 6.
  - Sektorspecifikke hensyn
  - Fleksibilitet i lyset af trusselsbilledet mv.
  - Modifikation: Minimumsimplementering

Eksempler fra ”modelbekendtgørelsen”

- ”Politik for risikoanalyse”, jf. lovforslagets § 6, stk. 1, nr. 1:
- metoder til at identificere og analysere kendte og forudsigelige risici mod sikkerheden i enhedens net- og informationssystemer
- metoder til identifikation, vurdering, håndtering og prioritering af passende risikostyringsforanstaltninger
- Kriterier for vurdering og evaluering af risici
- En beskrivelse af risikoejers rolle og ansvar
- En beskrivelse af ledelsens rolle og ansvar og
- Dokumentation af risikostyringsarbejdet, herunder dokumentation af implementering af risikostyringsforanstaltninger og begrundelse for enhedens accept af restrisiko

- **NB:** Det bliver næppe mere konkret end dette.

Leverandørstyring

Leverandørstyring – ”lovforslagets akilleshæl”

§ 6, stk. 1, nr. 4:

”Foranstaltningerne skal som minimum omfatte eller tage højde for:

…

Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.”

Fra NIS 2-direktivets præambel 56:

”Små og mellemstore virksomheder er i stigende grad mål for angreb i forsyningskæden på grund af deres mindre strenge foranstaltninger til styring af cybersikkerhedsrisici og angrebsstyring, samt det faktum at de har begrænsede sikkerhedsressourcer. Sådanne angreb i forsyningskæden har ikke kun indvirkning på små og mellemstore virksomheder og deres aktiviteter isoleret set, men kan også have en kaskadevirkning på større angreb på enheder, som de leverede varer til.”

Leverandørstyring – ”lovforslagets akilleshæl”

Fra NIS 2-direktivets præambel 86:

”Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere.”

Leverandørstyring – ”lovforslagets akilleshæl”

Modelbekendtgørelsen:

Fastsat i kapitel 5: ”Forsyningskædesikkerhed”

Krav om (ikke udtømmende):

1) Risikobaseret tilgang i jeres politik for leverandørforhold
2) Procedurer for at identificere og vurdere risici, ”der er specifikke for hver direkte leverandør og tjenesteudbyder i forsyningskæden.”
3) Kriterier for udvælgelse af og kontraktindgåelse med direkte leverandører og tjenesteudbydere.
4) Metoder til at vurdere den generelle kvalitet og modstandsdygtighed af de leverede produkter og tjenester.
5) Metoder til at vurdere direkte leverandører og tjenesteudbyderes cybersikkerhedspraksis.

Leverandørstyring – ”lovforslagets akilleshæl”

Hvad betyder alt dette i praksis?:

1) Leverandør- og kontraktstyring er centralt i NIS 2, og vil blive mere vanskeligt end databehandleraftaler efter GDPR.
2) Uanset hvilke krav lovforslaget og bekendtgørelserne ender med at indeholde, vil den grundlæggende øvelse følge de rammer, der er beskrevet ovenfor.
3) Det afgørende er, at I får rettet fokus mod de største cyberrisici i jeres leverandørkæde. Den juridiske compliance øvelse bliver så;
    1) at I kan dokumentere jeres til- og fravalg i den forbindelse, begrundelsen herfor, hvilke planer I har lagt for at adressere de mangler, I afdækker mv.
    2) at jeres ledelse kan betrygges om, at de – ofte vanskelige – prioriteringer I har foretaget er forsvarlige såvel juridisk som cybersikkerhedsfagligt.
    3) at I får indgået nye aftaler med jeres leverandører/kunder. Opgavens omfang spejler naturligvis antallet og modenheden af jeres leverandører/kunder.
    4) ”Den sidste forsvarslinje” – Hav dokumentationen på plads, og husk hvor myndighederne kommer fra…

Hændelseshåndtering

Hændelseshåndtering – et studie i formålet med NIS 2

Lovforslagets § 12 – tidlig varsling og hændelsesunderretninger

Tidlig varsling[1]

Væsentlige og vigtige enheders skal give ”tidlig varsling” til CSIRT og den kompetent myndighed om ”væsentlige hændelser” inden for 24 timer:

En hændelse anses for at være væsentlig, hvis

1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller

2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

[1] CSIRT (Computer Security Incident Response Teams)

Hændelseshåndtering – et studie i formålet med NIS 2

Hændelsesunderretning

En hændelsesunderretning, skal give:

1) en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger,

2) sendes uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse.

Hændelseshåndtering – et studie i formålet med NIS 2

Endelig rapport

En endelig rapport sendes senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde følgende:

a) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning.

b) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.

c) Anvendte og igangværende afbødende foranstaltninger.

d) De eventuelle grænseoverskridende virkninger af hændelsen.

NB: Ordlyden af denne bestemmelser er endelig.

Konklusion om hændelseshåndtering

- Al erfaring viser, at netop hændelseshåndtering indebærer nogen af de største risici.

- Kravene i NIS 2-loven er på dette punkt særdeles omfattende, og forudsætter modenhed og indsigt i håndteringen af trusler mv. Det vil udfordre de fleste.

- Samtidig viser § 12 meget klart, hvad NIS 2-loven handler om og hvem ansvaret nu væltes over på.

Nogle afsluttende råd

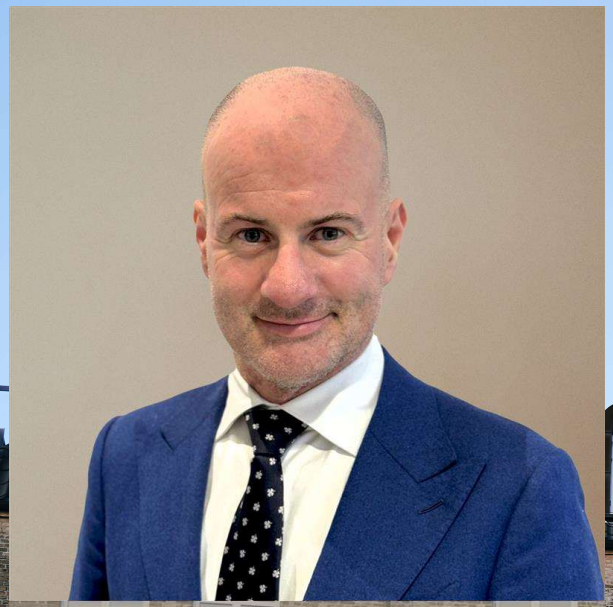
- Lad ikke NIS 2 blive ligesom visse GDPR-projekter, der var unødigt bebyrdende og ressourcekrævende, eller var styret af for overfladiske juridiske og it-faglige vurderinger. Det førte kun til frustrationer, og overlevede ikke mødet med driften og dagligdagen.
- Tag udgangspunkt i en konkret vurdering af cybertruslen i Jeres sektor, og hvordan den eksponerer jeres organisation. Dette indebærer, at man tidligt fokuserer på, hvor I er sårbare og sikrer, at governancekrav, leverandørkrav mv. adresserer de sårbarheder.
- Gå på begge ”ben”.
- Ressourcetrækket håndteres bedst ved at front-loade med fokus på korrekt afgrænsning af scope, trusselsvurdering og jura. Derefter vil meget give sig selv.
- Guld, sølv eller bronze?

CO:PLAY

LAW · TECHNOLOGY · BUSINESS

Spørgsmål?

Tøv ikke med at tage fat i mig



Christian Wiese Svanberg
Partner

E-mail: cws@coplay.law
Telefon: +45 2275 2646