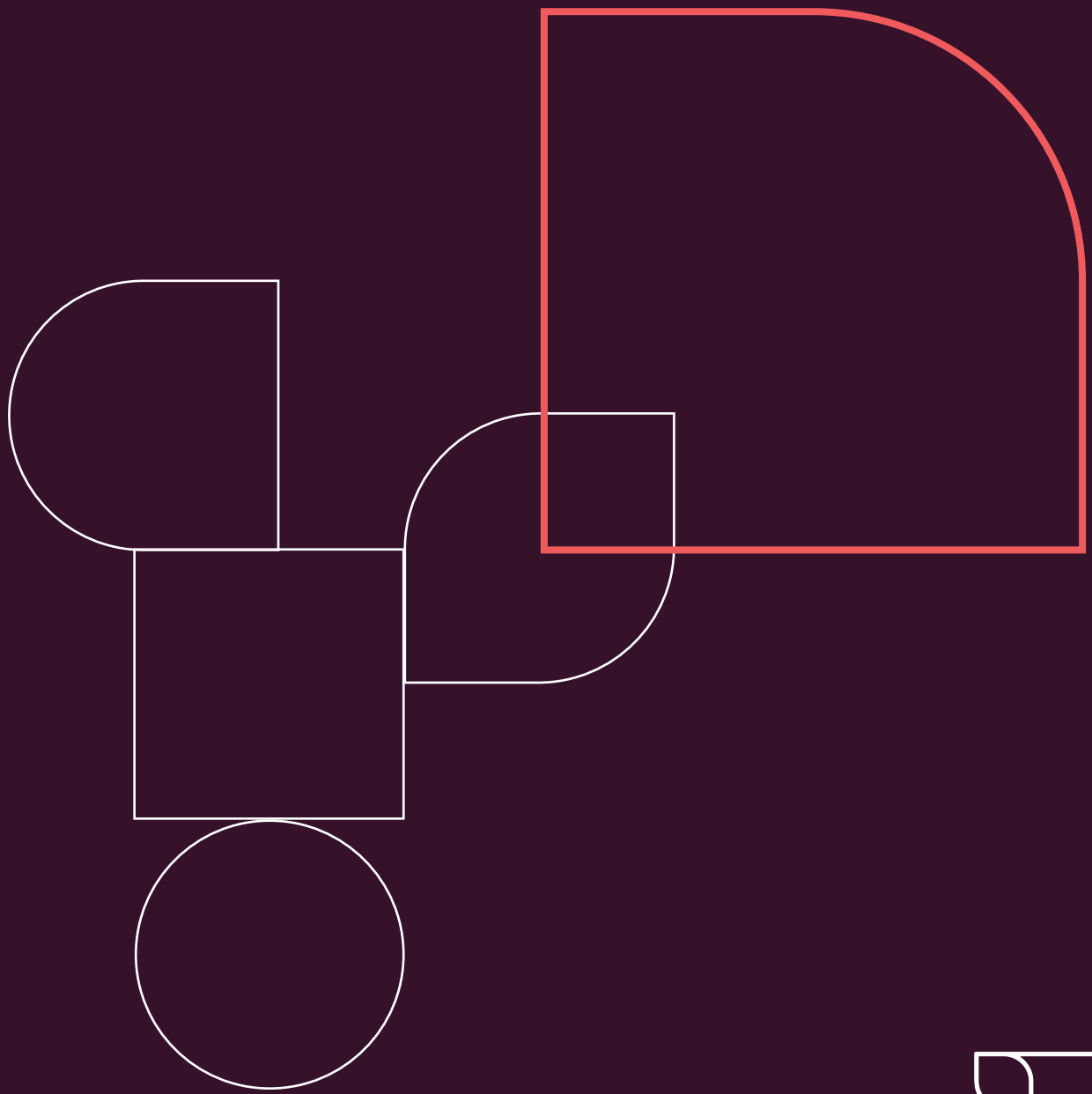
13 RIGTIGE

IT-BRANCHENS ANBEFALINGER TIL IMPLEMENTERING AF NIS2



ITB.DK

IT·BRANCHEN

IT-Branchens NIS2-udspil

Omkring 1.400 danske virksomheder bliver snart ramt af nye massive it-sikkerhedskrav fra EU, da de med et nyt EU-direktiv, NIS2, pludselige bliver defineret som en del af den kritiske infrastruktur.

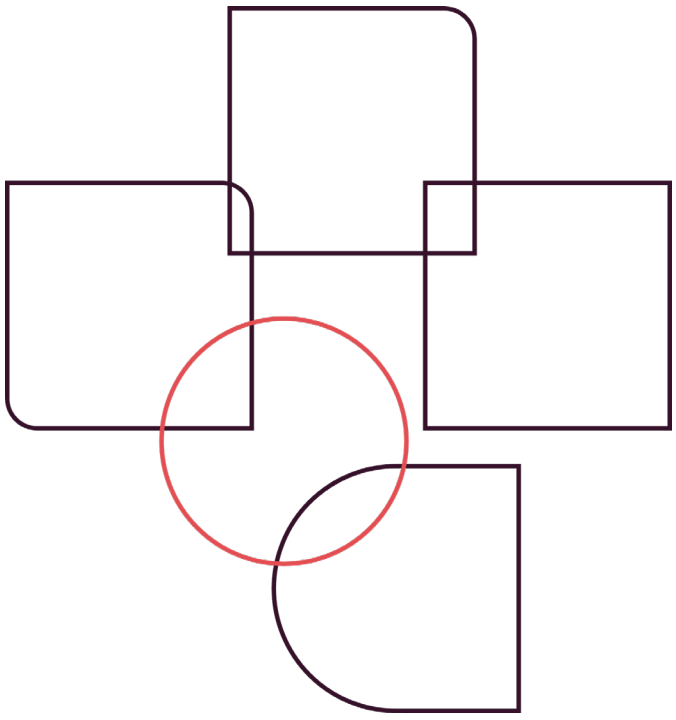
Tidligere har blot 130 danske virksomheder været en del af den kritiske danske infrastruktur. Nu bliver bl.a. dele af detailhandlen samt en række fødevareproducenter, restauranter og transportvirksomheder også defineret som en del af den kritiske infrastruktur.

Det betyder, at de skal leve op til de omfattende it-sikkerhedskrav, som NIS2-direktivet kommer med.

Men de færreste af de ramte virksomheder er sandsynligvis klar over det, og en stor del af Danmarks kritiske infrastruktur risikerer derfor ikke at være klar til hverken direktivet, der træder i kraft allerede i oktober 2024, eller fremtidens cybertrusler.

Det er derfor vigtigt, at vi både lovgivningsmæssigt, organisatorisk og i forhold til implementeringen i virksomhederne sikrer, at vi i Danmark opnår en effektiv, rettidig og hensigtsmæssig implementering af EU's NIS2-direktiv.

IT-Branchen har derfor samlet en række anbefalinger, der skal sikre en succesfuld implementering af NIS2-direktivet i Danmark og på tværs af de berørte brancher.



NIS2

NIS2-direktivet er en massiv udfordring

En analyse foretaget af IRIS Group på vegne af Industriens Fond, der kortlægger 12 ud af de 18 sektorer, der forventes at blive omfattet af NIS2, viser, at mere end 1.000 danske virksomheder og organisationer skal forholde sig til NIS2.

Medregnes de resterede 6 sektorer, hvor usikkerheden ift. omfattede virksomheder og organisationer er større pga. manglende dansk lovgivning, vurderes antallet af virksomheder og organisationer samlet at blive langt højere. En tidligere analyse udarbejdet af IT-Branchen med hjælp fra Danmarks Statistik kortlagde, at NIS2 omfatter ca. 1.400 virksomheder.

Det er væsentlig flere end de nuværende ca. 130 virksomheder og organisationer, der er omfattet af NIS1. Hertil indeholder NIS2 en række skærpede krav til forsyningskædesikkerhed, hvilket betyder, at en masse underleverandører til de omfattede virksomheder også vil blive afkrævet at skulle leve op til et højere niveau af cybersikkerhed.

Dårligt udgangspunkt

Analysen fra IRIS Group på vegne af Industriens Fond viser, at mere end 70% af de adspurgte virksomheder i mindre grad eller slet ikke lever op til de kommende NIS2-krav.

Mere end hver femte af virksomhederne er fortsat i tvivl om, hvorvidt de vil blive berørt af direktivet.

Manglende indsigt i direktivet

Mere end hver fjerde SMV har slet ikke sat sig ind i direktivets indhold. For store virksomheder er det hver tiende.

Blandt de virksomheder der har forsøgt at sætte sig ind i direktivet, fordi de vurderer, at de bliver omfattet af direktivet, har hver femte i mindre grad eller slet ikke en plan for at leve op til dets krav.

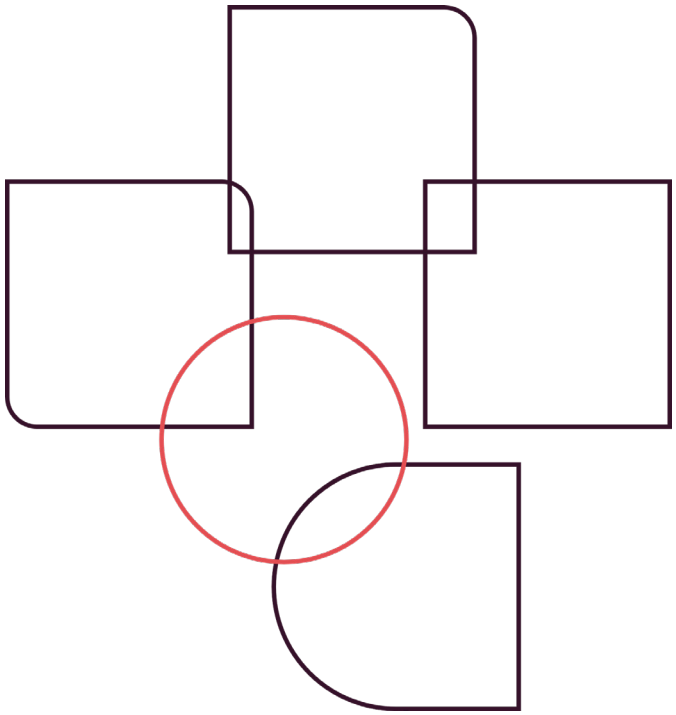
Uvished medfører handlingslammelse

Netop det, at virksomhederne endnu ikke har vished om, hvorvidt de bliver omfattet af NIS2, gør virksomhederne handlingslammede, viser analysen, og it-virksomhederne er blandt de virksomheder, hvor uvisheden er størst.

Mere end 40% af de adspurgte it-virksomheder i analysen er således i tvivl om, hvorvidt de bliver omfattet af direktivet.

Derfor scorer it-sektoren også lavt i analysen, når det kommer til andelen af virksomheder, der har sat sig ind i direktivet og har en plan klar for implementering af de påkrævede it-sikkerhedsforanstaltninger.

Kigger man omvendt kun på de virksomheder, der har sat sig ind i direktivet og/eller vurderer at blive omfattet af direktivet, ligger it-sektoren over gennemsnittet ift., hvor stor en andel af virksomhederne, der er klar til at imødekomme direktivets krav.



Anbefalinger til lovgivning og organisering

Som analysen fra IRIS Group og Industriens Fond viser, kan uvished om direktivets scope og omfattede virksomheder medføre uhensigtsmæssig inaktivitet blandt virksomhederne.

IT-Branchen opfordrer derfor til, at Forsvarsministeriet i samarbejde med de ansvarlige ressortmyndigheder hurtigst muligt kortlægger og adviserer de endeligt NIS2-omfattede virksomheder, så virksomhederne kan afsætte tid og ressourcer til at træffe de nødvendige foranstaltninger og blive klar til at imødekomme direktivets krav inden oktober 2024.

Såfremt arbejdet med lovgivningen trækker ud, bør de virksomheder, der med sikkerhed er omfattet af NIS2, adviseres, også før den endelige lovgivning er vedtaget.

1 Fælles rammelovgivning og ens krav

Det nuværende NIS1 direktiv, som omfattede syv sektorer, er i dag implementeret jfr. sektoransvarsprincippet via 13 forskellige bekendtgørelser.

Følges den samme fremgangsmåde med NIS2, kan slutresultatet bliver mere end 30 forskellige bekendtgørelser.

IT-Branchen anbefaler, at der udarbejdes en fælles rammelovgivning, som i passende omfang respekterer sektoransvarsprincippet, men også er operationel og sørger for, at sektorernes tiltag er sammenlignelige, passer til risici, afspejler sektorernes interdependens og kan rapporteres på en fælles form.

2 Begrænsning i antal nye CSIRT'er

IT-Branchen anbefaler, at der arbejdes på etablering af fælles CSIRT'er og herunder afklares, om der er flere sektorer, der kan operere under samme myndighed mhp. bl.a. at opnå en højere grad af omkostningseffektivitet, undgå unødig mangel på og udvanding af kompetencer samt unødig forsinkelse i implementeringen hos myndighederne.

Dette vurderes fint at kunne fungere sammen med de nuværende CSIRT'er, der allerede er etableret i forbindelse med NIS1.

3 Samarbejde om etableringen af CSIRT'er

IT-Branchen anbefaler, at etableringen af CSIRT'er skal ske i samråd med berørte brancher og med mulighed for finansieringsbidrag. Der skal også være en kompetent tilsynsmyndighed.

Dertil bør det overvejes, hvilke opgaver myndighederne med fordel kan udlicitere til private cybersikkerhedsaktører for at understøtte og fremme offentlig-privat samarbejde på cybersikkerhedsområdet.

4 Ensartet myndighedstilsyn

IT-Branchen anbefaler, at der etableres et ensartet myndighedstilsyn, der sikrer, at virksomheder, der opererer i mere end én omfattet sektor, ikke bliver mødt af tilsyn fra flere forskellige myndigheder, der stiller forskelligartede krav og forpligtelser.

Virksomhederne skal kunne nøjes med at forholde sig til én tilsynsmyndighed eller at tilsynsmyndighederne samordner deres arbejde.

5 Fælles tilsynskoncept

IT-Branchen anbefaler ligeledes, at der udarbejdes et fælles tilsynskoncept, som sikrer, at sektorerne kan sammenlignes, og at der automatisk kan opsamles data på tværs af sektorerne til en samlet national vurdering af risici og compliance.

6 Harmonisering af NIS2 på europæisk plan

IT-Branchen opfordrer også til, at Danmark bidrager til at sikre koordination og harmonisering ift. implementeringen af NIS2 på europæisk plan, så de virksomheder, der er aktive i andre EU-lande, ikke rammes af forskellige krav, men kan bruge samme tilgang til compliance på tværs af alle landene.

7 Balanceret dansk implementering

NIS2 direktivet er et minimumsdirektiv. Det vil sige, at de enkelte medlemsstater kan vælge at implementere yderligere eller at skærpe krav.

IT-Branchen anbefaler, at eventuel skærpelse af krav overvejes nøje ift. risikoen for at danske virksomheder stilles dårligere i konkurrence med virksomheder fra andre

medlemsstater.

8 Koordinering med anden regulering

IT-Branchen anbefaler, at der sikres samspil med andre reguleringstiltag inden for sikkerhedsområdet, som enten er vedtaget eller undervejs, så de samme foranstaltninger kan understøtte flere lovgivninger.

9 Kortlægning af foranstaltninger

IT-Branchen opfordrer til, at der fra myndighederne udarbejdes en kortlægning af foranstaltninger bl.a. ift. ISO-standarder og andre relevante standarder, så harmonisering af implementeringen understøttes.

Der skal samtidig etableres et fælles ensartet begrebsapparatet, der anvendes af alle omfattede enheder.

Dette bør koordineres med det pågående arbejde i ENISA vedr. en operationalisering af kravene i artikel 21 til NIS2-direktivet.

10 Kommuner skal omfattes af NIS2

IT-Branchen opfordrer til, at de danske kommuner omfattes af NIS2, så direktivet kan bruges som løftestang til et kærkomment løft af cybersikkerheden i kommunerne, og der samtidig sker en harmonisering af niveauet af cybersikkerhed på tværs af hele den offentlige sektor (stat, regioner og kommuner).

Anbefalinger til implementering i virksomhederne

EU forventer, at de virksomheder, der skal leve op til det nye NIS2-sikkerhedsdirektiv skal øge deres it-investeringer med 20-30%.

For de danske virksomheder anslår analysevirksomheden IDC, at hver virksomhed i gennemsnit vil få en merudgift på 350.000 kr., hvilket svarer til samlede ekstra it-investeringer for de 1.400 berørte virksomheder på 448 mio. kr.
Lever virksomheden ikke op til NIS2-direktivet, risikerer de samtidig bøder på op til 75 mio. kr. eller 2% af virksomhedens omsætning – alt efter hvad der er højest.

11 Rettidig vejledning til virksomhederne

Analysen lavet af IRIS Group og Industriens Fond viser yderligere, at virksomhederne i høj grad efterspørger styrket vejledning om eksisterende og ny regulering samt adgang til best practise cases.

Det er vigtigt, at vejledningen kommer snarest så virksomhederne har den tilgængelig i forbindelse med deres implementering af NIS2.

IT-Branchen opfordrer derfor til, at der hurtigst muligt udarbejdes en praktisk vejledning om, hvorledes NIS2-kravene efterleves og implementeres. Vejledningen skal bl.a. omfattende følgende:

- NIS2 direktivet stiller direkte krav til ledelsens involvering i arbejdet omkring cybersikkerhed. IT-Branchen opfordrer til, at det præciseres, hvordan begrebet "ledelsesorgan" skal forstås i en dansk kontekst, dvs. en præcisering af de personer og organer i ledelsen, som skal godkende og føre tilsyn med cybersikkerhedsrisici.

- De direkte omfattede virksomheder skal have hjælp til fortolkning af implementeringslovgivningen, gerne med udgangspunkt i konkrete eksempler. Virksomhederne skal understøttes i prioriteringen af sikkerhedstiltag ud fra risiko- og væsentlighedsvurderinger. Dette kan f.eks. suppleres af en 10-punktliste med basale cybersikkerhedstiltag, der adresserer minimumskravene i NIS2 og som bringer virksomheden godt i retning af overholdelse af direktivet.

- Der skal være særligt fokus på at rådgive virksomhederne omkring kravene til forsyningskædesikkerhed, herunder hvilke typer af underleverandører, der skal stilles krav til, hvilke krav de skal stille samt, hvordan overholdelse af kravene dokumenteres i forhold til myndighedstilsyn f.eks. via anvendelse af certificeringer og/eller eksterne (revisions)audits.

- Leverandører til direkte omfattede virksomheder skal ligeledes have klar vejledning om konsekvenserne af NIS2 og implementering af nødvendige foranstaltninger, f.eks. i forhold til ansvarsfastlæggelse og eventuel genforhandling af kontrakter med NIS2-omfattede kunder mv.

12 Positive effekter af NIS2

Cybersikkerhed er ikke kun et lovkrav, men i stigende grad også et krav fra samarbejdspartnere, kunder og investorer. Industriens Fonds cyberbarometer viser bl.a. at bedre cybersikkerhed styrker virksomhedernes konkurrencefordele i form af effektivitet og nytænkning, øget tillid og bundlinje.

IT-Branchen tilskynder derfor til, at der i den generelle kommunikation til virksomhederne også lægges vægt på de positive effekter af en øget cybersikkerhed frem for et ensidigt fokus på de negative konsekvenser af manglende efterlevelse af NIS2.

13 Anvendelse af D-mærket

IT-Branchen anbefaler, at der samarbejdes med D-mærket, så det bliver et konkret værktøj til at hjælpe virksomhederne med at leve op til de anførte minimumsforanstaltninger i NIS2 (sammen med øvrige relevante standarder og certificeringer som fx ISO 27001).

Vi skaber et digitalt Danmark med mennesket i centrum

IT-Branchen er Danmarks største brancheorganisation for it- og televirksomheder. Vi hjælper hver dag branchen og samfundet med at vokse.

I IT-Branchen brænder vi for at skabe et digitalt samfund for alle. Et samfund i vækst, og hvor Danmark står som et globalt fyrtårn, fordi vi udnytter teknologien til gavn for klimaet, økonomien og det enkelte menneske. Det gavner Danmark, erhvervslivet, den enkelte borger og vores medlemsvirksomheder.

LÆS MERE OM OS PÅ ITB.DK

IT·BRANCHEN