Næringslivets sikkerhets-råd

Arbeidsnotat:

Høringsinnspill til digitalsikkerhetsforskriften

Norge er et land som i økende grad er avhengig av digital infrastruktur og tjenester. Dette gjør oss sårbare for digitale trusler og angrep, og det er derfor avgjørende med et robust og effektivt regelverk for digital sikkerhet. Implementeringen av EUs NIS-direktiv i norsk lov er et viktig skritt i denne retningen. Næringslivets Sikkerhetsråd er derfor grunnleggende positiv til loven og forskriftens formål om å «sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester».

Vi er imidlertid bekymret for at loven, og fremtidige EU-reguleringer, kan føre til et stort og uoversiktlig antall tilsynsmyndigheter innen digital sikkerhet. NSR tror tilsynsmyndigheten som hovedregel bør legges til et sentralt kompetansemiljø, og bare unntaksvis til sektorvise tilsynsmyndigheter. Man bør også vurdere om ulike tilsynsoppgaver innenfor teknologi, personvern og digital sikkerhet bør samles i Datatilsynet eller et nytt teknologi- og personverntilsyn.

Næringslivets Sikkerhetsråd mener også at det er behov for enkle og tydelige retningslinjer og mekanismer for varsling og rapportering av digitale sikkerhetshendelser. Det bør tydeliggjøres hva som regnes som en hendelse, og lages veiledninger til hvordan rapportering skal gjøres. Dette vil bidra til å redusere unødvendig ressursbruk og gjøre prosessen mer oversiktlig for virksomhetene. Et sentralt rapporteringspunkt vil også forenkle denne rapporteringsprosessen.

Næringslivets Sikkerhetsråd har 10 konkrete innspill til digitalsikkerhetsforskriften:

1. Risiko for fragmentert tilsynsregime om digital sikkerhet

Justis- og beredskapsdepartementet foreslår at myndigheter med sektoransvar skal føre tilsyn etter digitalsikkerhetsloven i sin sektor. Nasjonal sikkerhetsmyndighet foreslås å være tilsynsmyndighet der det ikke er etablert et sektortilsyn, samt å ha en koordinerende og veiledende rolle overfor de øvrige tilsynsorganene.

Næringslivets Sikkerhetsråd er bekymret for hvordan tilsynsmyndigheten skal organiseres i praksis. Vi mener dette må utredes og beskrives tydeligere. Selv om digitalsikkerhetsloven

foreløpig har et begrenset virkeområde, innenfor sektorer med relativt tydelige sektormyndigheter, er vi bekymret for at det skapes organisatorisk presedens som kan skape utilsiktet presedens på sikt – særlig i forbindelse med innføringen av NIS2-direktivet i Norge.

Innføringen av nye EU-krav innebærer at en digital hendelse i fremtiden vil kunne få minst fire berøringspunkter inn mot myndighetene og ulike tilsynsorgan:

a) **Sektorvis rapporteringsplikt**, for eksempel etter storulykkeforskriften, kraftberedskapsforskriften, rammeforskriften/styringsforskriften, forskrift om sikring av havneanlegg, finanstilsynsloven, med mer.

b) **Datatilsynet** skal varsles ved brudd på personopplysningssikkerheten, etter personvernforordningen artikkel 33.

c) **Nye EU-krav om rapportering/tilsyn**. EUs KI-forordning (AI act) krever utpeking av tilsynsmyndigheter. Direktoratet for økonomistyring (DFØ) anbefaler i rapport 2024:9 å utpeke NKOM som nasjonalt kontaktpunkt og koordinerende myndighet, og at minst 12 sektorvise tilsyn gis nye tilsynsoppgaver knyttet til kunstig intelligens. Andre fremtidige direktiver og forordninger fra EU (eksempelvis Digital Service Act og Critical Entities Resilience Directive) vil trolig også komme med krav om ulike rapporterings- og tilsynsordninger.

d) **Varsling og rapportering etter digitalsikkerhetsloven**.

For noen få bransjer med tydelig definerte sektorvise tilsynsmyndigheter (for eksempel finanssektoren), er det etter vår oppfatning et ønske fra bedriftene at flest mulig tilsynsoppgaver samles til sektortilsynet som kjenner bransjen best. Forslaget til digitalsikkerhetslov ivaretar dette behovet.

For store deler av næringslivet er imidlertid denne organiseringen utfordrende. For det første fordi det i mange bransjer ikke finnes en åpenbar kandidat til å være sektorvis tilsynsmyndighet. Denne utfordringen vil bli ekstra synlig når lovens virkeområde på sikt skal utvides i tråd med NIS 2. Eksempelvis er verken Mattilsynet eller Konkurransetilsynet etter vår og bedriftenes vurdering særlig egnet til å bli tilsynsorgan for digital sikkerhet i en stadig mer høyteknologisk matbransje. En annen utfordring for mange bedrifter, særlig i industrien, er at de er underlagt mange ulike tilsynsmyndigheter. Departementet foreslår at virksomheter som opererer i flere sektorer, skal forholde seg til flere tilsynsmyndigheter om digital sikkerhet. Det tror vi vil bli svært krevende i praksis. For disse næringslivsaktørene vil det være en bedre løsning med et sentralisert og spesialisert tilsyn på digital sikkerhet.

Som minimum må det etableres en standardisert tilsynsmetodikk på tvers av tilsynsorganer, som vil bidra til en mer enhetlig tolkning av kravene.

Næringslivets Sikkerhetsråd er også bekymret for at loven, og kommende forordninger og direktiver fra EU, vil føre til at det må etableres et stort antall nye kompetansemiljøer på digital sikkerhet i de ulike sektortilsynene. Det er allerede stor etterspørsel etter kompetanse på digital sikkerhet, og vi antar det vil bli både dyrt og krevende å rekruttere det personellet man trenger til de

ulike tilsynene. Man risikerer å ende opp med mange små og grunne kompetansemiljøer, som vil konkurrere med andre offentlige virksomheter og bedrifter om en knapphetsressurs.

Det er også en risiko for at ulike tilsynsmyndigheter vil utføre tilsyn på ulike måter, kreve ulik dokumentasjon, og i verste fall sanksjonere ulikt på tvers av sektorer.

Næringslivets Sikkerhetsråd mener på bakgrunn av dette at hovedregelen bør være ett sentralt tilsyn, men med en unntaksmulighet der departementene ved behov kan delegere tilsynsmyndighet til sektorvise tilsyn etter god dialog med den berørte bransjen.

Næringslivets Sikkerhetsråd mener også at departementet bør vurdere den overordnede strukturen på tilsynene knyttet til digital sikkerhet, for å sikre at nye EU-krav løses helhetlig. I stedet for at tre ulike tilsyn/direktorat skal løse tre lignende oppgaver, bør det vurderes å rendyrke ett overordnet teknologi- og personverntilsyn for personopplysninger, kunstig intelligens, og digital sikkerhet.

Konkret endringsforslag til forskriften:

Eksisterende § 20 første ledd	*Ansvarlig departement utpeker myndighet som skal føre tilsyn med virksomheter innenfor egen sektor. For virksomheter uten tilsynsmyndighet er Nasjonal sikkerhetsmyndighet tilsynsmyndighet.*
Nytt forslag § 20 første ledd	*Nasjonal sikkerhetsmyndighet er tilsynsmyndighet. Ansvarlig departement kan ved behov utpeke myndighet som skal føre tilsyn med virksomheter innenfor egen sektor.*

2. Innmeldingskrav for underlagte virksomheter

Justis- og beredskapsdepartementet foreslår at virksomheter som omfattes av loven selv plikter å melde inn ulike opplysninger til Nasjonal sikkerhetsmyndighet (NSM) og tilsynsmyndigheten(e) i de sektorene virksomheten opererer i. Departementet ber spesifikt om høringsinnspill på dette, og antyder to alternativer: 1) At virksomheten kun får krav om å melde seg til NSM, og at NSM utfører videreformidling av informasjonen til tilsynene, og 2) at offentlige myndigheter utpeker (og varsler) virksomheter som underlegges forskriften.

NSR vurderer det som akseptabelt at virksomhetene selv må forstå at de er underlagt lovens virkeområde. Et system med utpeking av virksomheter, etter samme metode som etter Sikkerhetsloven, vil etter NSRs syn bare bidra til å forsinke og byråkratisere implementeringen av loven.

Næringslivets Sikkerhetsråd mener plikten til å melde inn opplysninger bør avgrenses til Nasjonal sikkerhetsmyndighet eller én sentral tilsynsmyndighet. Fra bedriftenes perspektiv vil det, som beskrevet i forrige punkt, kunne bli krevende å manøvrere blant ulike tilsyn som har krav på opplysninger. For å sikre forutsigbarhet og enkel gjennomføring, bør derfor bedriftene kun gis plikt til å melde inn opplysninger til ett kontaktpunkt.

Konkret endringsforslag til forskriften:

Eksisterende § 5 første ledd	*Tilbyder av en samfunnsviktig tjeneste skal snarest melde inn til Nasjonal sikkerhetsmyndighet og tilsynsmyndigheten opplysninger om*
Nytt forslag § 5 første ledd	*Tilbyder av en samfunnsviktig tjeneste skal snarest melde inn til Nasjonal sikkerhetsmyndighet eller tilsynsmyndigheten opplysninger om*

3. Behov for unntakshjemmel for forskriftens krav

Det bør etableres en unntakshjemmel for å gi dispensasjon til forskriftens krav, for eksempel knyttet til OT-miljøer, der krav om for eksempel oppdatering av programvare ikke er aktuelt.

Konkret endringsforslag til forskriften:

Ny paragraf i kapittel 3 eller 4	***Dispensasjon*** Tilsynsmyndigheten kan gi dispensasjon fra kravene i kapittel 3 dersom det foreligger særlige grunner, det er sikkerhetsmessig forsvarlig, og er i tråd med bransjestandarder eller lignende.

4. Risiko for reaktivt rapporteringsfokus på bekostning av håndtering

Vi er bekymret for at lovverket binder seg for strengt til et reaktivt rapporterings- og tilsynsfokus i en hendelsesfase, på bekostning av mer proaktive mekanismer gjennom hendelseshåndtering i rammen av CERT/SRM og anmeldelse/etterforskning fra politiet. Flere av NSRs medlemsbedrifter er også bekymret for at ressursbruk til rapportering simultant med en pågående hendelse, kan gå ut over hendelseshåndteringen, særlig i den kritiske fasen de første 24 timene.

Forholdet mellom de operative miljøene og tilsynsmyndigheten bør også beskrives tydeligere, særlig for Nasjonal sikkerhetsmyndighet, som har både en tilsynsrolle og en operativ rolle.

Næringslivets Sikkerhetsråd mener også at varslings- og rapporteringsplikten bør begrenses til én instans.

Konkret endringsforslag til forskriften:

Eksisterende § 17 første punktum	*Varsel etter digitalsikkerhetsloven § 8 og § 11 skal gis til tilsynsmyndigheten med kopi til Nasjonal sikkerhetsmyndighet.*
Nytt forslag § 17 første punktum	*Varsel etter digitalsikkerhetsloven § 8 og § 11 skal gis til tilsynsmyndigheten eller til Nasjonal sikkerhetsmyndighet.*

5. Forskriftens forhold til etablerte standarder om digital sikkerhet

Harmonisering av krav på tvers av sektorer og nordiske land vil redusere friksjonen for etterlevelse for virksomheter med partnere eller virksomhet i flere sektorer eller land. Vi er bekymret for at forskriftens særnorske, detaljerte krav kan skape forvirring. Vi anbefaler at man i stedet knytter

kravene til etablerte standarder og rammeverk, eksempelvis ISO 27001 eller NSMs grunnprinsipper. Disse standardene vil også være mer dynamiske med tanke på oppdaterte krav for å håndtere ny risiko og nye problemstillinger. Dette forslaget krever en omfattende omskriving av hele forskriftens kapittel 2.

Forskriften behandler ikke risikoaksept, eller andre former for å ta kalkulert risiko. I digitalsikkerhetsloven står det at «Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen». Denne lovteksten åpner, slik vi tolker det, for at virksomhetene kan utvise en form for risikoaksept basert på hensiktsmessighet eller proporsjonalitet. Dette poenget er ikke hensyntatt i forskriften.

6. Styrets ansvar for digital sikkerhet

Vi mener styrets ansvar for digital sikkerhet må gjøres tydeligere.

Konkret endringsforslag til forskriften:

Eksisterende § 6 siste ledd	*Virksomhetens leder har ansvar for at virksomheten har et forsvarlig sikkerhetsnivå innenfor virkeområde til digitalsikkerhetsloven. Sikkerhetsstyringssystemet skal godkjennes av virksomhetens leder og gjennomgås minst årlig med sikte på å forbedre virksomhetens sikkerhetsarbeid.*
Eksisterende § 6 siste ledd	*Virksomhetens styre har ansvar for at virksomheten har et forsvarlig sikkerhetsnivå innenfor virkeområde til digitalsikkerhetsloven. Sikkerhetsstyringssystemet skal godkjennes av virksomhetens leder og gjennomgås minst årlig med sikte på å forbedre virksomhetens sikkerhetsarbeid.*

7. Forskriftens forhold til OT og IOT

Det er uklart om forskriftens krav også gjelder for OT og IOT. Dette er beskrevet for dårlig.

Dette punktet må beskrives bedre.

8. NSMs rolle

Nasjonal sikkerhetsmyndighet gis flere roller i den nye forskriften. Vi er urolige for hvordan disse oppgavene skal balanseres/segregeres. Dette bør også vurderes av det pågående Gjerdrem-utvalget, som skal vurdere NSMs oppgaver og organisering.

Forskriften legger opp til at NSM skal være:

- Koordinerende og veiledende rolle for alle tilsynsmyndigheter.
- Tilsynsmyndighet der det ikke er utpekt et sektortilsyn.
- Nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemet
- Nasjonalt responsmiljø for håndtering av hendelser.
- Veiledningsansvar.

9. Bekymring for åpen deling av sårbarheter og kritisk informasjon

Virksomheter som rammes av betydelige hendelser får etter den nye forskriften plikt til å rapportere betydelige mengder sensitiv informasjon til myndighetene. Informasjonen man skal rapportere er sensitiv, både av hensyn til sikkerhet og forretningsdrift. NSRs medlemsbedrifter er særlig bekymret for eksponering av sårbarheter og nye angrep mens hendelser pågår. Enkelte fageksperter mener at det bør gå 90 dager før informasjon om en hendelse slippes, for å unngå at hendelsen utnyttes. Bedriftene påpeker også at det må etableres et system for tydelig merking av sensitivitet og informasjonsdeling.

Næringslivets Sikkerhetsråd mener forskriften i betydelig større grad burde erkjent at den informasjonen virksomheten plikter å rapportere på, eller må gi innsyn i under et tilsyn, som hovedregel er å anse som sensitiv og taushetsbelagt informasjon. Etter vår vurdering vil denne type informasjon være unntatt offentlighet etter offentleglova §§ 13 og 24.

Konkret endringsforslag til forskriften:

Eksisterende § 18 første ledd	*Når det er innenfor digitalsikkerhetslovens formål og i den utstrekning det er nødvendig, kan varslingsmottaker dele med andre aktører taushetsbelagt informasjon mottatt ved varsling.*
Forslag til ny § 18 første ledd	*Informasjon om sårbarheter og forretningskritiske forhold, som virksomheten rapporterer eller gir innsyn i under tilsyn, regnes som taushetsbelagt. Når det er innenfor digitalsikkerhetslovens formål og i den utstrekning det er nødvendig for å forhindre ytterligere alvorlige hendelser, kan varslingsmottaker dele med andre aktører taushetsbelagt informasjon.*

10. Sikkerhetskrav til underleverandører

Flere bedrifter opplever at kravene til leverandørstyring er uklare, og at avgrensningen på hvilke leverandører som må inngå i risikostyringen er uklart. Det oppleves usikkerhet rundt hvor langt ned i leverandørkjeden virksomheter er forpliktet til å kontrollere etterlevelse av kravene hos leverandørene. Det uttrykkes også bekymring rundt utfordringene rundt omfanget av dette, både for virksomheten selv og for leverandørene.