Næringslivets sikkerhets-råd

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 Oslo

Næringslivets Sikkerhetsråds høringsinnspill til digitalsikkerhetsforskriften

Vi viser til Justis- og beredskapsdepartementets brev av 11. september 2024 (24/3567 – ODTV), med anmodning om innspill til høring på forslag til forskrift til lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven).

Næringslivets Sikkerhetsråd (NSR) er en stiftelse eid av NHO, Virke, Spekter, Rederiforbundet og Finans Norge, og har rundt 300 større bedrifter i Norge som medlemmer. Stiftelsens formål er å ivareta næringslivets fellesinteresser innen sikkerhet og beredskap, særlig knyttet til tilsiktede trusler.

Innføringen av digitalsikkerhetsloven med tilhørende forskrift blir et tidsskille for digital sikkerhet i Norge. Næringslivets Sikkerhetsråd er positiv til formålet om å ha grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet. Samtidig ser vi noen utfordringer med hvordan departementets forslag til forskrift skal gjennomføres i praksis, i møte med et dynamisk og komplekst fagområde. Noen av disse problemstillingene peker departementet selv på i høringsbrevet, og vi er glade for den tydelige invitasjonen til å gi innspill.

NSR har følgende hovedinnspill til forslaget til ny digitalsikkerhetsforskrift:

1. Hver enkelt virksomhet bør bare være forpliktet til å forholde seg til én myndighetsaktør for varsling, rapportering og tilsyn etter digitalsikkerhetsforskriften.

2. Forskriftens detaljerte tekniske krav vil i mange tilfeller ikke kunne etterleves. Det er derfor behov for enten mer funksjonsrettede krav, og/eller en unntakshjemmel.

3. Informasjon som deles gjennom rapportering og tilsyn vil i stor grad være sensitiv, og bør tydeligere beskrives som taushetsbelagt i forskriften.

Vi mener digital sikkerhet best kan oppnås gjennom etterlevelsesprinsippet og god veiledning, og forutsetter at tilsynsmyndigheten får ressurser til å ivareta dette på en hensiktsmessig måte.

Næringslivets Sikkerhetsråd erkjenner at forskjellige bransjer og bedrifter har ulike behov og meninger om hvordan forskriften bør utformes. Vi har derfor anstrengt oss for å identifisere næringslivets minste felles multiplum, gjennom en omfattende medvirkningsprosess fra sikkerhetsmiljøet i næringslivet. I prosessen har vi fortløpende testet hypoteser og posisjoner på bedriftene for å avdekke eventuelle motforestillinger, og dermed også oppnådd konsensus om de tre hovedinnspillene.

Underveis i medvirkningsprosessen har vi blant annet gjennomført en større workshop i samarbeid med PwC, der nøkkelpersoner i 84 store og sentrale bedrifter bidro til å identifisere problemstillinger og bekymringer. Vi har også gjennomført en spørreundersøkelse blant NSRs medlemmer, der 78 nøkkelpersoner (primært ledere innen sikkerhet og IT) har avgitt svar. Spørreundersøkelsen ga mange interessante og viktige svar, og kan om ønskelig oversendes til departementet i sin helhet. Momenter fra workshopen, undersøkelsen og en rekke samtaler med eksperter fra blant annet Netsecurity, mnemonic, PwC og andre bedrifter ligger også til grunn for høringsinnspillet.

Selv om digitalsikkerhetsloven foreløpig bare omfatter en relativt liten del av næringslivet, opplever vi et sterkt engasjement fra bedrifter som trolig vil underlegges digitalsikkerhetsloven om noen år, når NIS2 skal innføres i Norge. Vår oppfatning er at de valg og prinsipper departementet går inn for i forskriften nå, etter alt å dømme vil få implikasjoner for disse bedriftene på sikt. Vi ber derfor departementet ta hensyn til de langsiktige effektene av forskriften, for ikke å gjøre valg som vil være uheldige og irreversible når lovens virkeområde utvides.

Detaljert innspill:

1. Ønskelig med kun ett kontaktpunkt for varsling, rapportering og tilsyn

Departementet 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. Virksomheter som opererer innen flere sektorer skal ifølge departementet melde inn til samtlige tilsynsvirksomheter i sektorene de opererer i, samt til Nasjonal sikkerhetsmyndighet.

Departementet foreslår også 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.

Basert på svært tydelige tilbakemeldinger fra sikkerhetsmiljøet i næringslivet er Næringslivets Sikkerhetsråd bekymret for at virksomhetene i fremtiden vil få for mange kontaktpunkter for varsling, rapportering og tilsyn om digital sikkerhet. Det kan føre til uklarheter, ulikheter og byråkrati. For å unngå dette mener NSR at hver virksomhet bare bør forpliktes til å forholde seg til én myndighetsaktør for varsling, rapportering og tilsyn etter digitalsikkerhetsforskriften.

Bekymringen er basert på ulike forhold:

- Noen bransjer, for eksempel finans, helse, olje- og gass, og kraft, har et tydelig sektortilsyn, der det allerede er etablert kompetansemiljøer for digital sikkerhet. Etter vår oppfatning ønsker bedriftene i disse bransjene at flest mulig tilsynsoppgaver samles til sektortilsynet som kjenner deres bransje best, slik det legges opp til i departementets forslag til forskrift. NSR støtter dette, og mener sektorvise tilsyn vil fungere godt i disse konkrete bransjene. Det oppleves imidlertid som unødvendig og byråkratiserende at disse bedriftene også skal rapportere til Nasjonal sikkerhetsmyndighet, i tillegg til sin sektorvise tilsynsmyndighet.

- I mange bransjer finnes det imidlertid ingen tydelig sektorvis tilsynsmyndighet. Dette gjelder særlig for bransjer som ligger an til å bli lagt inn under loven når virkeområdet skal utvides etter NIS 2-direktivet, for eksempel matbransjen. Her finnes det ikke et tydelig eller velegnet sektorvis tilsyn for digital sikkerhet. NSR kjenner bransjen godt gjennom et nyetablert cybersikkerhetssamarbeid i matbransjen (CYMAT), der bedrifter som Tine, Nortura, Orkla, NorgesGruppen, Coop og Rema 1000 deltar. I dag er disse selskapene ikke lenger matbedrifter med litt teknologi, men heller teknologibedrifter som håndterer mat – med robotiserte lagre, autonome ferjer, komplekse digitale logistikksystemer, nettbutikker og digitale kundeløsninger. En sentral tilsynsmyndighet vil være den beste løsningen for matbransjen og andre bransjer uten en tydelig sektorvis tilsynsmyndighet.

- 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. Myndighetenes sektorvise tilnærming treffer ikke alltid næringslivet klokkerent, noe som fører til at mange bedrifter i praksis kan bli underlagt utilsiktet mange sektorvise tilsynsmyndigheter. I NSRs undersøkelse oppgir hele 65 prosent at de er underlagt tre eller flere tilsynsmyndigheter.
    - Eksempel fra en større industribedrift: De kan forvente tilsyn fra Direktoratet for samfunnssikkerhet og beredskap (fordi de er underlagt storulykkeforskriften), fra Næringslivets sikkerhetsorganisasjon (fordi de er industrivernpliktige), fra Kystverket (fordi fabrikken har et ISPS-havneanlegg), fra Luftfartstilsynet (fordi de er sikkerhetsgodkjent for flyfrakt), Miljødirektoratet og statsforvalteren (fordi de er underlagt miljøregelverket), og så videre. Fabrikkens havneanlegg og flyfraktfasiliteter vil trolig falle innenfor digitalsikkerhetsforskriftens virkeområde. Med et prinsipp om sektorvise tilsynsmyndigheter vil derfor både Kystverket og Luftfartstilsynet ha interesser i industribedriftens digitale sikkerhet.
    - Et annet eksempel fra et transportselskap, som drifter både busser, hurtigbåter, ferjer og trikk. Hurtigbåtene og ferjene vil ha et passasjergrunnlag som kommer innenfor terskelen i digitalsikkerhetsforskriften, og vil trolig få Sjøfartsdirektoratet som sektorvis tilsyn. Trikken omfattes også av forskriften, og her er det formodentlig Statens jernbanetilsyn som vil være sektorvis tilsynsmyndighet.

  NSR er bekymret for at mange bedrifter i praksis vil få tre til fire varslings- og rapporteringspunkter med et sektorvis tilsynsprinsipp. Det er også uklart hvor avgrensningen eventuelt skal gå mellom disse tilsynene, og hvor mye av bedriftens IT-infrastruktur – som i stor grad er felles for hele bedriften – skal være underlagt forskriftens krav, når bare deler av virksomheten omfattes. For disse bedriftene mener NSR det vil være bedre med én sentral tilsynsmyndighet.

- Departementets forslag innebærer 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. Én sentral tilsynsmyndighet vil trolig være mer kosteffektiv, og bidra til at man får ett sterkt, sentralt fagmiljø – i stedet for mange små.

- Næringslivets Sikkerhetsråd er bekymret for at kommende forordninger og direktiver fra EU vil føre til ytterligere tilsynsmyndigheter med krav om varsling og rapportering. EUs KI-forordning (AI act) krever eksempelvis utpeking av tilsynsmyndigheter. Direktoratet for økonomistyring (DFØ) anbefaler i rapport 2024:9 å utpeke Nasjonal kommunikasjonsmyndighet 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.

- Det er fare for at ulike tilsynsmyndigheter vil utføre tilsynsrollen på ulike måter, kreve ulik dokumentasjon, og i verste fall sanksjonerer ulikt på tvers av sektorer. Som minimum må det etableres en standardisert tilsynsmetodikk på tvers av tilsynsorganer, som vil bidra til en mer enhetlig tolkning av kravene.

Det er ikke usannsynlig at en bedrift i fremtiden må utføre lovpålagt varsling og rapportering om digital sikkerhet til minst fire-fem instanser:

1) tap av personopplysninger til Datatilsynet,
2) hendelser med kunstig intelligens til Nkom,
3) til én eller flere sektorvise tilsynsmyndighet,
4) til Nasjonal sikkerhetsmyndighet.

I tillegg kommer frivillig varsling til sektorvise responsmiljø/CERT, Nasjonalt cybersikkerhetssenter ved NSM, og anmeldelse til politiet. For bedriftene vil det bli komplisert å navigere mellom alle disse varslingsaktørene – særlig når NSM både skal ha en tilsynsrolle med *lovpålagt* varslingsplikt, og en rolle som nasjonalt responsmiljø for håndtering av hendelser med *frivillig* varsling.

Næringslivets Sikkerhetsråd er bekymret for at den lovpålagte varslingsplikten knytter seg for strengt til et reaktivt rapporterings- og tilsynsfokus i en hendelse, og går på bekostning av frivillige og mer proaktive varslingstiltak til responsmiljøer og politiet. At næringslivet inngir anmeldelser er svært viktig for å ivareta vår kollektive sikkerhet, fordi politiet på bakgrunn av anmeldelse kan iverksette etterforskning og ta i bruk tvangsmidler for å hindre videre straffbare handlinger.

Flere av NSRs medlemsbedrifter er også bekymret for at ressursbruk til rapportering til flere ulike aktører kan gå ut over hendelseshåndteringen, særlig i den kritiske fasen de første 24 timene. NSR vil også trekke frem Regjeringens digitaliseringsstrategi, som understreker behovet for tverrsektoriell situasjonsforståelse og bred nasjonal koordinering for å stå imot dagens

sammensatte trusselbilde. Vi tror dette vil bli vanskelig å oppnå, hvis tilsynsmyndigheten spres på så mange sektorvise tilsyn.

Næringslivets Sikkerhetsråd mener derfor at det som hovedregel bør være ett sentralt tilsyn etter digitalsikkerhetsloven. Departementene bør likevel ha mulighet til å delegere tilsynsmyndighet til sektorvise tilsyn der det allerede finnes kompetansemiljøer på digital sikkerhet, og et sektorvis tilsyn er ønsket av den aktuelle bransjen.

Vi vurderer det som akseptabelt at virksomhetene selv må forstå at de er underlagt lovens virkeområde, etter et etterlevelsesprinsipp. Et system med utpeking av virksomheter, etter samme metode som etter sikkerhetsloven, vil etter vårt syn bare bidra til å forsinke og byråkratisere implementeringen av loven. Plikten til å melde inn opplysninger bør som tidligere nevnt avgrenses til én aktør – enten til et sentralt tilsyn, eller til et unntaksvis utpekt sektorvis tilsyn.

Næringslivets Sikkerhetsråd vil i tillegg oppfordre Regjeringen til å gjøre en overordnet vurdering av tilsynsstrukturen for personvern, teknologi og digital sikkerhet, og se dette i sammenheng med EU-krav som er under innføring i norsk rett. Vi tror det kan være fornuftig å vurdere et felles tilsyn for personopplysninger, kunstig intelligens, og digital sikkerhet, i stedet for at Datatilsynet, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, og en rekke sektortilsyn skal løse disse oppgavene hver for seg.

Konkrete endringsforslag til forskriften:

- § 20 første ledd: Hovedregelen bør være ett sentralt tilsyn, men med en unntaksmulighet der departementene ved behov kan delegere tilsynsmyndighet til sektorvise tilsyn.
- § 5 første ledd: Innmeldingsplikten bør bare gå til én aktør.
- § 17 første punktum: Varslings- og rapporteringsplikten bør begrenses til én aktør.

2. Behov for funksjonsrettede krav og/eller unntaksbestemmelse

Av de spurte bedriftene er 96 prosent svært positive eller positive til innføringen av digitalsikkerhetsloven med forskrifter. Sikkerhetsmiljøet i næringslivet opplever de foreslåtte kravene som fornuftige og akseptable. Dersom man i dag etterlever kravene til eksempelvis ISO 27001 eller NSMs grunnprinsipper, ser det også ut til at man i stor grad vil etterleve de foreslåtte kravene i forskriften.

Sikkerhetsmiljøet i næringslivet gir samtidig flere eksempler på at forskriftens krav ikke alltid vil kunne etterleves: For eksempel vil det være krevende å oppfylle kravet om oppdatert programvare i operasjonell teknologi (OT), særlig i gamle, frittstående systemer som ikke lenger oppdateres fra leverandøren. Eksempler på dette er styringssystemer på fartøy, isolerte produksjonssystemer i et industrianlegg, og frittstående medisinsk utstyr på et sykehus. Slike sårbare OT-systemer sikres på andre måter, for eksempel ved å isolere dem helt fra internett, eller ved å «pakke dem inn» i sikre nettverkssegmenter med god tilgangsstyring, overvåkning, og andre sikkerhetsmekanismer. ISA 62443 er et eksempel på en internasjonal standard for digital sikkerhet for slike produksjonssystemer.

Næringslivets Sikkerhetsråd mener det må være mulig å fravike forskriftens krav i slike tilfeller, og at det derfor bør legges inn en unntaksbestemmelse i forskriften.

Vi tror unntaksbestemmelsen bør baseres på et egenerklæringsprinsipp, der virksomheten må dokumentere unntaket og hvilke tilsvarende sikkerhetsløsninger man i stedet har valgt – for eksempel bransjestandarder eller internasjonale standarder som nevnte ISA 62443. Unntaksbestemmelsen bør etter vårt syn ikke organiseres som en godkjenningsordning. Det vil kreve stor saksbehandlingskapasitet og teknisk kompetanse hos tilsynsmyndigheten, og vil kunne føre til en ansvarsfraskrivelsespraksis hos virksomheten.

Et alternativ til å etablere en unntaksbestemmelse, er å endre kravene i forskriften fra *detaljkrav* til *funksjonskrav*. Virksomhetene vil da stå friere til å bruke metoder, teknologi, erfaring og kreativitet til å oppfylle sikkerhetskravene – så lenge funksjonene etterleves.

Næringslivets Sikkerhetsråd tror også at forskriften bør beskrive risikoaksept, altså hvilken kalkulert risiko man har rom for å ta. 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 og proporsjonalitet. Dermed vil de viktigste systemene kunne prioriteres sikkerhetsmessig, på bekostning av mer perifere systemer der konsekvensen er lav ved utfall.

De internasjonale standardene ligger i stor grad til grunn for større bedrifters digitale sikkerhetsarbeid i dag. Slike standarder vil alltid være mer dynamiske og oppdaterte enn en nasjonal forskrift, og vil raskere kunne tilpasse krav til ny risiko og nye problemstillinger. Standardene er også internasjonalt anerkjent og utbredt, og en rekke norske bedrifter bruker i dag ulike styringssystem og verktøy tilpasset standardene for å avdekke avvik, prioritere hvilke avvik som er mest kritiske, og automatisere rapportering. Næringslivets Sikkerhetsråd mener at bedrifter som etterlever NSMs grunnprinsipper eller internasjonale standarder ikke må avkreves et ytterligere kontroll- og dokumentasjonsregime basert på forskriftens særnorske krav. Dette vil i praksis bare føre til økt byråkratisering og «papir-sikkerhet», ikke reell styrking av den digitale sikkerheten.

Konkrete endringsforslag til forskriften:

- Ny paragraf med unntakshjemmel etter egenerklæringsprinsippet.

3. Sårbarheter og hendelser er taushetsbelagt 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 en deling av denne type informasjon betinge at aktuelle tilsynsorgan gjør bruk av offentleglovas kapittel 3 for å unnta saken fra offentligheten.

Konkrete endringsforslag til forskriften:

- §18 første ledd: Informasjon om sårbarheter og forretningskritiske forhold, som virksomheten rapporterer eller gir innsyn i under tilsyn, må regnes som taushetsbelagt, og bør i hovedsak kun deles i den utstrekning det er nødvendig for å forhindre ytterligere alvorlige hendelser.

Øvrige kommentarer

I tillegg til de tre hovedinnspillene, vil Næringslivets Sikkerhetsråd kommentere enkelte andre forhold som sikkerhetsmiljøet i næringslivet har påpekt:

- Styret og ledelsens ansvar bør tydeliggjøres i forskriftens § 6. Det er styrets, ikke leders, ansvar at virksomheten har et forsvarlig sikkerhetsnivå. Samtidig er det virksomhetens ledelse, ikke bare leder, som bør være ansvarlig for å godkjenne sikkerhetsstyringssystemet.

- Nasjonal sikkerhetsmyndighet gis flere roller og oppgaver i den nye forskriften. Næringslivets Sikkerhetsråd er bekymret for hvordan disse oppgavene skal balanseres, segregeres og ressurssettes. De nye oppgavene NSM får etter forskriften bør vurderes av det pågående Gjerdrem-utvalget, som skal vurdere NSMs oppgaver og organisering.

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

- 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.

- 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. Optimalt hadde man etablert en felles varslingstjeneste på nett, der man i én innmelding kunne varslet alle berørte myndigheter. I en slik tjeneste burde det også vært mulig for frivillig å huke av for å anmelde saken til politiet.