



Justis- og beredskapsdepartementet
Postboks 8005 Dep.
0030 OSLO

VÅR REFERANSE
18/13492

DERES REFERANSE

DATO
28.03.2019

Høringssvar: NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet

Det vises til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2018 med to saker på felles høring:

1. Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018: 14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.
2. Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

Høringssvaret omfatter Finanstilsynets vurderinger av konsekvensene av forslagene for henholdsvis foretakene i finanssektoren og Finanstilsynet som forvaltningsorgan.

IKT-sikkerhetsutvalgets anbefalinger

Ny nasjonal lov om IKT-sikkerhet

Finanstilsynet støtter utvalgets forslag om å utrede en ny nasjonal lov om IKT-sikkerhet. Finanssektoren er omfattet av felles krav til IKT-sikkerhet fastsatt i IKT-forskriften¹. Forskriften stiller blant annet krav knyttet til risikohåndtering, sikkerhet, avviks- og endringshåndtering, samt varsling. Dette er områder utvalget mener bør inngå i en fremtidig nasjonal lov om IKT-sikkerhet. Finanstilsynet mener at utvalgets foreslåtte områder ivaretas i det eksisterende regelverket for finanssektoren. En lovgivning i tråd med IKT-sikkerhetsutvalgets anbefalinger antas dermed å ha begrensede konsekvenser for finanssektoren.

Finanstilsynet legger IKT-forskriften til grunn også for egen virksomhet. En lovgivning som stiller krav tilsvarende IKT-forskriften for offentlig forvaltning, vil imidlertid medføre en ny plikt for Finanstilsynet.

Krav om IKT-sikkerhet ved alle offentlige anskaffelser

¹ Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften)

Finanstilsynet støtter utvalgets forslag om krav om IKT-sikkerhet ved alle offentlige anskaffelser. IKT-forskriftens § 6, som stiller krav om at sikkerhet skal ivaretas ved anskaffelser, synes i hovedsak å ivareta utvalgets forslag til krav om IKT-sikkerhet ved alle offentlige anskaffelser.

Nasjonalt IKT-sikkerhetssenter

Finanstilsynet ser det som positivt at det etableres et nasjonalt IKT-sikkerhetssenter for å ivareta behovet for nødvendig koordinering og informasjonsutveksling mot ulike sektorer og etablerte responsmiljøer.

Foretakene i finanssektoren har etter IKT-forskriften en plikt til å rapportere alvorlige eller kritiske sikkerhetshendelser (og operasjonelle hendelser) til Finanstilsynet.

Tydeligere regulering av og ansvar for tilkoblede produkter og tjenester

Finanstilsynet mener at krav til helhetlig ansvar for sikkerhet ved tilkoblede produkter og tjenester innen finanssektoren er ivaretatt gjennom IKT-forskriften, da forskriftens virkeområde omfatter IKT-systemer som er av betydning for foretakets virksomhet (§1 andre ledd).

Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet
Finanstilsynet støtter utvalgets forslag.

Utkast til lov som gjennomfører NIS-direktivet

Finanstilsynet har ikke merknader til Justis- og beredskapsdepartementets utkast til lov som gjennomfører NIS-direktivet. Lovutkastet omfatter tilbydere av samfunnsviktige tjenester og digitale tjenester, og vil dermed ikke gjelde for offentlig forvaltning. Lovutkastet medfører derfor ikke noen nye krav for intern IKT-forvaltning i Finanstilsynet. I punktene nedenfor er Finanstilsynets vurderinger av konsekvenser for finanssektoren knyttet opp mot de spørsmål som er stilt i høringsbrevet.

1. I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring og internkontroll?

Etter Finanstilsynets vurdering har det over lengre tid vært arbeidet systematisk med IKT-sikkerhet i finansnæringen, i tråd med gjeldende regelverk. Finanstilsynet stiller konkrete krav om risikostyring og internkontroll i finanssektoren gjennom Forskrift om risikostyring og internkontroll². Gjennom *Veiledning til forskrift om risikostyring og internkontroll* har Finanstilsynet beskrevet risikostyring basert på rammeverket COSO³.

Banker og forsikringsselskap er unntatt ovennevnte regelverk, og krav om sikkerhetsstyring og internkontroll reguleres derfor gjennom annet lovverk. For banker (med unntak av Norges Bank, jf. Finansforetaksloven⁴ §1-6) stiller finansforetaksloven krav om at det skal etableres *forsvarlige styrings- og kontrollsystemer*. I tillegg stilles det krav gjennom hhv. finansforetaksloven og

² FOR-2008-09-22-1080 - Forskrift om risikostyring og internkontroll

³ Helhetlig risikostyring – et integrert rammeverk (COSO2, 2004/2005 på norsk v. Norges Interne Revisorers Forening

⁴ LOV-2015-04-10-17 - Lov om finansforetak og finanskonsern (Finansforetaksloven)

finansforetaksforskriften⁵ om at styret skal etablere et uavhengig kontrollorgan gjennom å ha internrevisjon eller ved at revisor gir en årlig bekreftelse til styret om risikostyringen og internkontrollen i virksomheten.

Det stilles i tillegg krav til sikkerhet og risikohåndtering gjennom IKT-forskriften.

Finanstilsynet stiller ikke krav om etterlevelse iht. fastsatte standarder og rammeverk, men registrerer at mange virksomheter selv velger å bli sertifisert innen ISO 9000-serien (ledelsessystem innen kvalitet) og ISO 27000-serien (ledelsessystem innen informasjonssikkerhet).

2. Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet

Finanstilsynet legger til grunn at en innføring av NIS-direktivet i norsk rett – slik det er gjort i utkast til lov om sikkerhet i nettverk og informasjonssystemer – ikke vil medføre konsekvenser for finansnæringen, da kravene i lovutkastet allerede er dekket av sektorspesifikke regelverk.

Finanstilsynet legger til grunn at nye IKT-sikkerhetskrav overfor tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester, kan bidra til en heving av IKT-sikkerheten som også kan være til nytte for finanssektoren.

3. Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet

En innføring av NIS-direktivet vil for Finanstilsynet medføre administrative og økonomiske kostnader forbundet med nye krav om rapportering, fordi IKT-sikkerhetshendelser som Finanstilsynet får melding om skal rapporteres videre. Finanstilsynet vurderer anslaget i høringsnotatet om økt arbeidsmengde på 0,25 årsverk til å være dekkende.

**4. Er din virksomhet per i dag underlagt krav til IKT-sikkerhet og varsling?
Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?**

Finanstilsynet viser til punkt 1.

5. Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?

Finanstilsynet viser til punkt 2.

⁵ FOR-2016-12-09-1502 - Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)

For Finanstilsynet

Per Mathis Kongsrud

direktør avdeling for digitalisering og analyse

Olav Johannessen

seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.