Vedlegg 2 til Skate-sak 1/2019

Sammendrag - Utdrag fra NOU 2018:14

1 Sammendrag

Liv og helse, demokrati og rettssikkerhet, økonomisk velferd og nasjonens suverenitet er viktige verdier som må beskyttes for å kunne opprettholde et trygt, fritt og velfungerende samfunn. Mange sider ved den teknologiske utviklingen kan styrke og bygge opp under disse verdiene. Teknologi kan for eksempel benyttes til å utvide helsetilbudet, bidra til effektivisering av virksomheter og gi nye måter for enkeltindivider å uttrykke seg på i sosiale medier.

Den teknologiske utviklingen gjør at det norske samfunnet i stadig større grad kobles sammen, og avhengighetene mellom virksomheter og mellom sektorer blir stadig sterkere. Norsk næringsliv og forvaltning har i tillegg stadig tettere bindinger til andre land. IKT-infrastrukturen representerer en stor og fortsatt økende samfunnsmessig verdi. Stadig mer informasjon lagres, transporteres og behandles digitalt, og nye tjenester, prosesser og produkter utvikles fortløpende. Den teknologiske utviklingen skaper nye og endrede risikoer og utfordringer som må håndteres.

Utvalget er gitt i oppdrag å vurdere om dagens regulering av IKT-sikkerhet er hensiktsmessig gitt de samfunnsutfordringene Norge står overfor. Utvalget er også bedt om å vurdere organiseringen av tverrsektorielt ansvar på IKT-sikkerhetsområdet. Ansvar, roller og oppgaver må være hensiktsmessig fordelt mellom etatene.

Utvalget legger tre overordnede prinsipper til grunn for sine anbefalinger. Arbeidet med IKT-sikkerhet må ha en risikobasert tilnærming som innebærer at vesentlig risiko prioriteres. Videre må IKT-sikkerhet balanseres opp mot brukervennlighet, økonomi og grunnleggende menneskerettigheter. En slik balanse innebærer at noe risiko må aksepteres for å oppnå økonomiske og sosiale mål. Til slutt krever arbeidet med IKT-sikkerhet en fleksibilitet i reguleringen og organiseringen slik at man kan tilpasse seg nye trusler, sårbarheter, teknologier og forretningsmodeller.

Nedenfor følger et sammendrag av utvalgets anbefalinger for å styrke den nasjonale IKT-sikkerheten. Utvalget står samlet bak anbefalingene.

1.1 Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Digitaliseringen av samfunnet gjør at virksomheter står overfor et stadig mer komplekst IKT-risikobilde. For at et digitalt samfunn som Norge skal fungere, er det nødvendig å minimere risikoen for at utilsiktede og tilsiktede hendelser rammer IKT-systemer. Til tross for potensielt betydelige økonomiske, sikkerhetsmessige og omdømmemessige konsekvenser har virksomheter ikke alltid tilstrekkelige insentiver til å beskytte seg mot digitale trusler.

Etter utvalgets vurdering håndteres ikke utfordringene på en hensiktsmessig måte i gjeldende regulering. En rekke lover og forskrifter stiller krav om IKT-sikkerhet. Det stilles imidlertid ikke alltid hensiktsmessige krav om sikring av IKT-systemer som understøtter virksomheters produksjon av varer og tjenester.

Gitt det gjeldende IKT-risikobildet mener utvalget at det må utarbeides en ny lov hvor det stilles krav om forsvarlig IKT-sikkerhet til alle samfunnskritiske virksomheter og offentlig forvaltning.

Den nye loven skal også gjennomføre NIS-direktivet i norsk rett. Kravene som følger av loven, må konkretiseres i forskrift og veiledning.

Utvalget mener at det ikke er nødvendig å sanere og harmonisere eksisterende regelverk før vedtakelse av loven. Det er viktigere å sørge for at det i fremtiden blir enhetlig begrepsbruk i lover og forskrifter som stiller krav om IKT-sikkerhet.

Selv om samfunnskritiske virksomheter og offentlig forvaltning har forsvarlig IKT-sikkerhet, gjenstår mange digitale sårbarheter. De fleste virksomheter er avhengige av lange og komplekse digitale verdikjeder. I prinsippet kan alle IKT-systemer bli benyttet som mellomledd i angrep mot andre egentlige mål, for eksempel samfunnskritiske virksomheter. Også tilkoblede produkter kan inngå i angrepsnettverk som kan skade samfunnskritiske funksjoner. Dette er risiko som i liten grad reduseres ved at det stilles krav om forsvarlig IKT-sikkerhet til samfunnskritiske virksomheter og offentlig forvaltning.

Utvalget har vurdert muligheten for å underlegge alle virksomheter krav om IKT-sikkerhet i lov, ikke bare samfunnskritiske virksomheter og offentlig forvaltning. Krav i lov kan være inngripende og ressurskrevende. Utvalget mangler konkrete holdepunkter for å si hvor stort det gjenstående behovet er for å styrke IKT-sikkerheten i alle norske virksomheter. Dersom behovet er stort, taler det for å stille krav i lov til alle norske virksomheter. Utvalget anbefaler derfor at det nedsettes et eget lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter.

1.2 Krav om IKT-sikkerhet ved anskaffelser

Anskaffelser av IKT-tjenester kan, og vil i mange tilfeller, gi bedre trygghet og mer stabile og tilgjengelige tjenester. Med andre ord kan anskaffelser av IKT-tjenester være et fornuftig IKT-sikkerhetstiltak.

Anskaffelser av slike tjenester er imidlertid ikke risikofritt. Det er utvalgets oppfatning at den største utfordringen med anskaffelser er manglende bevissthet om risikoen. For å kunne iverksette hensiktsmessige sikkerhetstiltak, er det avgjørende at virksomhetene vurderer risikoen ved alle anskaffelser. Virksomheter som blir omfattet av utvalgets forslag til ny lov om IKT-sikkerhet plikter å vurdere slik risiko.

Utvalget mener at det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Anskaffelsesregelverket bør endres slik at oppdragsgiveren får en slik plikt.

Statens standardavtaler (SSA) brukes av en rekke private virksomheter, i tillegg til offentlig sektor. Utvalget anbefaler at SSAene endres slik at IKT-sikkerhet blir tydeligere ivaretatt.

Det er et stort behov for kompetanse og veiledning om IKT-sikkerhet ved anskaffelser. Utvalget mener det er viktig at den eksisterende veiledningen på anskaffelsesområdet videreutvikles til å inkludere IKT-sikkerhet i større grad. Veiledningen om anskaffelser og SSAer bør samkjøres med annen veiledning om IKT-sikkerhet.

1.3 Etablere et nasjonalt IKT-sikkerhetssenter

Mange virksomheter opplever at råd og veiledning fra myndighetene er for lite koordinert mellom etatene. De er usikre på hvor de skal henvende seg når de har spørsmål om IKT-sikkerhet. Det er også utfordringer med koordinering og informasjonsdeling når uønskede digitale hendelser skal håndteres. Det er mange som etterlyser mer offentlig-privat samarbeid og en styrket innovasjonsevne innenfor IKT-sikkerhet. Det er behov for å samle kompetanse, skape synergier på tvers av sektorer og miljøer og gjøre samarbeidslinjene kortere og mer effektive.

Utvalget mener at etablering av et nasjonalt IKT-sikkerhetssenter er et godt grep for å møte dette behovet. Et senter kan være en pådriver for koordinering og samordning mellom sektorer og mellom offentlige og private aktører. Det kan være et sentralt kontaktpunkt for råd og veiledning til virksomheter, det kan koordinere håndtering av uønskede digitale hendelser og dele informasjon om trusler og sårbarheter.

Et IKT-sikkerhetssenter kan også tillegges oppgaver som ingen etater har ansvar for i dag, for eksempel å motta og offentliggjøre informasjon om digitale sårbarheter («Coordinated Vulnerability Disclosure»). Senteret må dessuten stimulere til mer forskning, utvikling og innovasjon.

Et nasjonalt IKT-sikkerhetssenter må ha en tydelig forankring i sivile myndigheter. Behovet for styrket IKT-sikkerhet er først og fremst knyttet opp mot sivile samfunnsfunksjoner og kritisk infrastruktur, både i offentlig og privat regi. Samtidig har forsvarssektoren en sentral rolle knyttet til statssikkerhet, og sivil og militær IKT-infrastruktur blir i økende grad integrert. Godt sivilt – militært samarbeid er derfor en viktig oppgave for senteret. Det er også nødvendig at et slikt senter har et tydelig grensesnitt mot nasjonalt cyberkrimsenter, som er under etablering i Kripos.

Parallelt med utvalgets utredning er det startet et arbeid med å etablere et nasjonalt cybersikkerhetssenter som del av NSM. Utvalget mener at det må ligge et godt beslutningsgrunnlag til grunn før det etableres et nasjonalt IKT-sikkerhetssenter i Norge. Justis- og beredskapsdepartementet, i samarbeid med Forsvarsdepartementet, må sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse. En slik analyse må baseres på en bred involvering av potensielle interessenter i privat og offentlig sektor. Behovsanalysen må avklare IKT-sikkerhetssenterets myndighetsforankring og kobling til NSM, og grensedragninger mot det planlagte nasjonale cyberkrimsenteret.

1.4 Tydelig regulering og ansvar for tilkoblede produkter og tjenester

Antallet produkter og tjenester som er koblet til internett er stort og i sterk økning. Manglende IKT-sikkerhet i slike produkter og tjenester kan utgjøre en trussel for forbrukere, virksomheter og samfunnssikkerheten.

Ansvaret for IKT-sikkerhet på dette området bør i større grad flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester.

Norge må videreføre sitt internasjonale samarbeid, særlig opp mot EU. Fordi mange tilkoblede produkter og tjenester brukes på tvers av landegrenser, er det viktig å ha et harmonisert regelverk internasjonalt. På denne bakgrunn mener utvalget at det er bedre å bidra til et oppdatert regelverk på EU-nivå enn at Norge unilateralt endrer regelverket på feltet.

Utvalget mener videre at det må være et tett samarbeid mellom tilsynsmyndigheter som Datatilsynet, Forbrukertilsynet, DSB og Nkom når det gjelder tilkoblede produkter og tjenester. Myndighetene må gi bedre råd og veiledning til importører, forhandlere og norske produsenter på dette området. Utarbeidelse av råd og veiledning må gjøres i samarbeid med bransjeaktørene. Målsettingen bør være å forebygge at produkter uten tilfredsstillende IKT-sikkerhet lanseres på det norske markedet, og å håndtere avdekkede sikkerhetshull på en god måte.

Myndighetene må også sørge for at produkter uten tilstrekkelig IKT-sikkerhet kan oppdages, varsles om og tilbakekalles. Forbrukerne må kunne heve kjøp av produkter og tjenester som ikke har tilstrekkelig IKT-sikkerhet.

Utvalget mener at myndighetsansvaret for IKT-sikkerheten i tilkoblede produkter og tjenester må tydeliggjøres. Det er viktig at DSB som produktsikkerhetsmyndighet holder seg oppdatert på utviklingen, og utvalget mener DSB bør få en tydelig rolle når det gjelder varsling, rapportering,

tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

1.5 Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

IKT-sikkerhet griper inn i alle sektorer og virksomheter i samfunnet. Denne kompleksiteten utfordrer styringen og samordningen av nasjonal IKT-sikkerhet.

Det foreligger ingen enkel oppskrift på hvordan myndighetene best mulig skal organisere seg for å møte disse utfordringene. Utvalgets informasjonsinnhenting har ikke avdekket noe åpenbart behov for å gjøre større endringer i ansvar, roller eller oppgaver til etatene. Det er imidlertid viktig at ansvarsforholdene er tydelig definert der det er tilgrensende områder, og at det er et godt og koordinert samarbeid på tvers av sektorer og etater.

Utvalget mener at Justis- og beredskapsdepartementet i større grad må være en synlig aktør som tar initiativ, løser opp i uklarheter, definerer mål, koordinerer og samordner arbeidet med nasjonal IKT-sikkerhet. Det er et politikkområde som bør løftes systematisk inn i styringsprosesser og i samfunnsdebatten. Etablering av et nasjonalt IKT-sikkerhetssenter og en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning vil styrke departementets evne til å utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.

Justis- og beredskapsdepartementet må ha en mer samordnet styring av underliggende etater når det gjelder IKT-sikkerhetsoppgaver. Utvalget mener også at Justis- og beredskapsdepartementet må være en tydelig pådriver for å samordne departementenes styringssignaler om IKT-sikkerhet.

Justis- og beredskapsdepartementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre, og at tilsyn med teknisk IKT-sikkerhet gis økt oppmerksomhet. Utvalget mener at samarbeidet som har funnet sted mellom en rekke etater og departementer innen HMS-tilsyn, er et godt eksempel på hvordan IKT-sikkerhetstilsyn kan koordineres.

NSM har en sentral rolle som Justis- og beredskapsdepartementets fagmiljø innenfor IKT-sikkerhet på sivil side. De understøtter også Forsvarsdepartementet i deres ansvar på IKT-sikkerhetsområdet i forsvarssektoren. Utvalget mener at Justis- og beredskapsdepartementet og Forsvarsdepartementet må gjennomgå modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes.