Vedlegg 1 til Skate-sak 1/2019
Mandatforståelse - Utdrag fra NOU 2018:14

2.2 Utvalgets mandatforståelse

Det er utarbeidet et omfattende kunnskapsgrunnlag på IKT-sikkerhetsområdet de siste årene, blant annet knyttet til digitale sårbarheter og hvilke trusler vi står overfor. Utvalget har tatt utgangspunkt i dette kunnskapsgrunnlaget i sitt arbeid. I tillegg har utvalget innhentet egne data spesielt knyttet til organisering og regulering. Se punkt 2.3 om utvalgets arbeid.

2.2.1 Begrepet IKT-sikkerhet

Begrepet IKT-sikkerhet har ikke en entydig definisjon. Det har grenseflater mot, eller oppfattes som synonymt med, informasjonssikkerhet, cybersikkerhet og digital sikkerhet. Innholdet i disse varierer og glir i noen grad over i hverandre. I noen dokumenter benyttes begrepene helt eller delvis synonymt, i andre tillegges de ulikt innhold. Innholdet i begrepet IKT-sikkerhet har endret seg noe over tid. Tradisjonelt har beskyttelse av nettverk og systemer vært vektlagt. I dag omfatter begrepet i større grad informasjonen som behandles i systemene og nettverkene samt tjenestene som systemene leverer.

IKT-sikkerhet forstås i denne utredningen som beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene. Sikkerhetsmålene for IKT-sikkerhet er

- tilgjengelighet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene er tilgjengelig der og når det trengs for brukerne
- integritet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene ikke endres utilsiktet eller uautorisert
- konfidensialitet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene kun er tilgjengelige for dem som rettmessig skal ha tilgang

Den enkelte virksomhet vil vekte sikkerhetsmålene ulikt ut fra hvilket formål den har eller skal understøtte, og hvilke krav og hvilket risikobilde den må forholde seg til. Basert på disse målene og vektingen av dem vil beskyttelsen omfatte teknologiske, menneskelige og organisatoriske barrierer, som skal motvirke uønskede digitale hendelser, evne til å oppdage slike hendelser og påfølgende reaksjon for å gjenopprette en sikker tilstand for IKT-systemene.

2.2.2 Forsvarlig nasjonal IKT-sikkerhet

Forsvarlig nasjonal IKT-sikkerhet er en overordnet målsetting i mandatet. Utvalget legger til grunn at bruken av ordet *nasjonal* innebærer IKT-sikkerhet som har betydning for samfunnet som helhet.

Med ordet *forsvarlig* forstår utvalget at det skal være et minimumsnivå på sikkerheten. Hva som må til for å oppnå et minimumsnivå, er imidlertid ikke entydig. Utvalget legger til grunn at forsvarlig IKT-sikkerhet kommer godt til uttrykk i NSMs grunnprinsipper for IKT-sikkerhet.[1] Disse bygger på anerkjente standarder og rammeverk i Norge og internasjonalt, og beskriver hva en virksomhet

[1] Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for IKT-sikkerhet*.

bør gjøre for å sikre sine IKT-systemer. En virksomhet som etterlever disse prinsippene, vil ha forsvarlig IKT-sikkerhet. Hovedpunktene i prinsippene er:[2]

1. Identifisere og kartlegge – gjør risikovurdering
2. Beskytte – sikre verdiene dine
3. Opprettholde og oppdage – vær bevisst
4. Håndtere og gjenopprette – lær av utfordringene dine

Hvert grunnprinsipp har underliggende teknologiske og organisatoriske sikringstiltak som beskriver hva som bør gjøres.

2.2.3 Regulering

Første del av mandatet omfatter å vurdere om dagens regulering er hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet.

Utgangspunktet for utvalget er at en regulering anses å stille krav om IKT-sikkerhet hvis den inneholder bestemmelser om beskyttelse av IKT-systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene.

Med begrepet *tverrsektorielt regelverk* forstås regelverk som stiller krav til offentlige og/eller private virksomheter i to eller flere samfunnssektorer. Utvalget har lagt til grunn at begrepet *regelverk* omfatter lov, forskrift og instrukser, mens begrepet *regulering* også omfatter *soft law* (standarder, bransjepraksis og veiledere). Eksempler her er NSMs grunnprinsipper, Difis og Datatilsynets veiledere om informasjonssikkerhet, og Normen i helsesektoren.[3]

2.2.4 Organisering

Andre del av mandatet innebærer å vurdere om Norge har en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet.

Utvalget legger til grunn at etater med tverrsektorielt ansvar har oppgaver som berører mer enn én statsråds sektoransvar, og har særlig vurdert følgende etater med tverrsektorielt ansvar på IKT-sikkerhetsområdet:

- Nasjonal sikkerhetsmyndighet (NSM)
- Direktoratet for samfunnssikkerhet og beredskap (DSB)
- Direktoratet for forvaltning og IKT (Difi)
- Nasjonal kommunikasjonsmyndighet (Nkom)
- Datatilsynet

NSM, DSB og Difi er de som tydeligst har tverrsektorielt ansvar.

Nkom er i utgangspunktet en sektormyndighet, men det elektroniske kommunikasjonsnettet (ekomnett) er en integrert del av den nasjonale IKT-infrastrukturen. For de fleste virksomheter er ekomnett og -tjenester også en integrert del av egne IKT-systemer. I et slikt perspektiv er Nkoms ansvarsområde tverrsektorielt, noe som også kommer til uttrykk i det utstrakte samarbeidet etaten har på sikkerhetsområdet med blant andre NSM og DSB.

[2]Hovedpunktene i grunnprinsippene samsvarer med hovedpunktene i veiledningen til NIS-direktivet som det britiske cybersikkerhetssenteret har utarbeidet, National Cyber Security Center (2018) *NIS Guidance Collection*.

[3]Normen i helsesektoren er et omforent sett av krav til informasjonssikkerhet basert på regelverket.

Datatilsynets oppgaver og kompetansefelt er tverrsektorielt i og med at personvernlovgivningen er allmenn og griper inn i alle sektorer. Datatilsynet skiller seg likevel fra de andre ved at det er et mer uavhengig organ som ikke instrueres av et departement. I vår tid er personvern uløselig knyttet til IKT-sikkerhet, og Datatilsynet er derfor en sentral aktør på dette området.

2.2.5 Øvrige avgrensninger

Det følger av mandatet at utredningen er avgrenset mot eksisterende sikkerhetslov og forslaget til ny sikkerhetslov. Med det mener utvalget at det ikke skal foreslås endringer i denne loven. Grensesnitt mellom sikkerhetsloven og regelverk på IKT-sikkerhetsområdet utenfor sikkerhetsloven er imidlertid beskrevet.

Utvalget har ikke vurdert organisering i politietaten eller Forsvaret. Følgende grensesnitt er i noen grad behandlet:

- mellom sivil sektor og forsvarssektor, herunder den gjensidige avhengigheten
- mellom politiet og relevante aktører når det gjelder IKT-kriminalitet
- mellom kommunalt og statlig nivå knyttet til IKT-sikkerhet