POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

NCIS Norway

Deres referanse:	Vår referanse:	Sted, dato
2018/05481	201803914-3	Oslo, 3. mars 2019

HØRINGSUTTALELSE – NOU 2018:14 OG UTKAST LOV FOR GJENNOMFØRING AV NIS-DIREKTIVET

Det vises til e-post mottatt 4. februar 2019 fra Politidirektoratet om Justis- og beredskapsdepartementets to saker for felles høring:

- Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018: 14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.

- Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

SAK 1 - NOU 2018:14

Utvalget har fem hovedanbefalinger:

1) Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
2) Det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser
3) Nasjonalt IKT-sikkerhetssenter
4) Tydeligere regulering av og ansvar for tilkoblede produkter og tjenester
5) Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet

Politidirektoratet ber særskilt om innspill på to av disse anbefalingene:

Kripos/

Post: Pb. 2094 Vika, 0125 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

Forslag om å etablere et nasjonalt IKT-sikkerhetssenter, og hvordan dette vil berøre politiets rolle og ansvar for ikt-sikkerhet eller eventuelt tilgrensende områder

Forslaget om å etablere et nasjonalt IKT-sikkerhetssenter er i det vesentlige omtalt i NOUen kapittel 17.

Å samle IKT-sikkerhetskompetanse kan være et gode for hele samfunnet. Det er allerede mangel på slik kompetanse i Norge, og det er enighet om at man trenger enda flere ressurser i fremtiden. Et samlet fagmiljø vil kunne bistå med å påse en tilstrekkelig IKT-sikkerhet, også innenfor politiets egensikringsbehov. Videre vil et kompetansesenter kunne gi IKT-teknisk støtte i etterretning og etterforskning av IKT-kriminalitet.

Når det er sagt er det viktig for Kripos å understreke at opprettelse av et IKT-sikkerhetssenter med tydelig koordineringsmekanisme for å håndtere alvorlige uønskede digitale hendelser, og etablering av et nasjonalt kontaktpunkt for IKT-sikkerhet mv. må bygge på eksisterende ansvarsfordeling.

Kripos er usikker på hvorvidt utvalget har lagt eksisterende ansvarsfordeling til grunn. Usikkerheten på dette punktet knytter seg i hovedsak til utvalgets uttalelser i pkt. 17.1.2 om "Organisering og Myndighetsforankring" hvor det avslutningsvis er anført følgende;

> *"Slik utvalget oppfatter det, er nasjonalt cyberkrimsenters formål etterforsking og påtale av straffbare handlinger, mens et IKT-sikkerhetssenter vil ha som formål å legge forholdene til rette for forsvarlig nasjonal IKT-sikkerhet...."*

Som det tydelig fremkommer i politiloven § 2 om "Politiets oppgaver" så strekker politiets ansvar seg langt ut over det å etterforske og påtale straffbare handlinger. Politiet skal i tillegg bl.a. beskytte person, eiendom og fellesgoder og verne om all lovlig virksomhet, opprettholde den offentlige orden og sikkerhet mv. Generelt skal politiet verne mot alt som truer den alminnelige tryggheten i samfunnet - enten alene eller sammen med andre myndigheter.

Etablering av et IKT-sikkerhetssenter må ta tilstrekkelig hensyn til gjeldende lovverk og sikre at grensene opp mot politiets oppgaver blir avklart også når det gjelder arbeidet med å forebygge, avdekke og håndtere digitale angrep. Dette er særlig viktig fordi flere av oppgavene som følger av politiloven § 2 ikke skal eller kan utføres av andre enn politiet – uavhengig av om utgangspunktet er digitalt eller fysisk.

Det kan i tillegg bemerkes at politiet har definert trygghet i det digitale rom som ett av fire strategiske hovedsatsingsområder i gjeldende virksomhetsstrategi, og det kan understrekes at trygghet i det digitale rom er en helt sentral komponent i politiets oppdrag. Dette er også et tydelig uttrykk for at innsatsområdet skal prege politiets prioriteringer fremover, noe f.eks. etableringen av nasjonalt cyberkrimsenter (NC3) ved Kripos har vist.

Generelt til forslaget om å opprette et nasjonalt IKT-sikkerhetssenter, og særlig til pkt. 17.1 som omhandler "Oppgaver og innretning", har Kripos funnet grunn til å stille spørsmål om politiets oppgaver og ansvar i tilstrekkelig grad er hensyntatt i utvalgets vurderinger og forslag.

Hvis man ser bort fra behovet for å avklare ansvarsforholdene mellom IKT-sikkerhetssenteret og NC3, er politiet oppgaver med det forebyggende IKT-sikkerhetsarbeidet ikke omtalt. Særlig

tydelig kommer dette til uttrykk i "*Figur 17.1 Et IKT-sikkerhetssenter som nasjonalt kontaktpunkt*" hvor politiet ikke en gang er nevnt som mulig deltaker i et fremtidig IKT-sikkerhetssenter. Hvordan utvalget først kan "glemme" politiets oppgaver innen dette området, og dernest synes å vurdere at den kunnskapen politiet besitter om IKT-kriminalitet ikke er relevant for et eventuelt IKT-sikkerhetssenter, er vanskelig å forstå.

Deteksjon, analyse og informasjonsdeling er sentrale momenter i enhver forebyggingsstrategi. For forebygging av IKT-kriminalitet er dette, etter Kripos' oppfatning, særlig relevant. Politiet er den myndigheten i Norge som har de beste forutsetninger, gjennom sitt oppdrag og mandat, til å være drivkraft og fasilitator for informasjonsdeling der alle sensorer for deteksjon av IKT-kriminalitet kan bidra innenfor et åpent og ugradert samarbeid. For Kripos er det også i denne sammenheng naturlig å vise til uttalelser fra mindretallet i Lysne I utvalget, i spørsmålet om "forbedret nasjonal operativ evne gjennom samlokalisering", som på side 273-275 fremfører vesentlige og gode poenger.

Senterets tiltenkte funksjoner inkluderer "å tilgjengeliggjøre oppdatert informasjon om trusler og sårbarheter", "være sentralt kontaktpunkt for råd- og veiledninger og ved uønskede digitale hendelser" samt "være pådriver for offentlig-privat samarbeid". Et aktuelt spørsmål vil i den sammenheng være hvilken informasjon som skal og ikke skal eller kan deles. I den kontekst er Kripos noe tvilende til hvorvidt de rammene EOS-tjenestene arbeider under, rent prinsipielt, er egnet til å drifte et svært bredt forankret senter som forutsetter aktiv informasjonsdeling. Det er samtidig relevant å stille seg spørsmålet om EOS-regelverket generelt er tilstrekkelig egnet til å dele og formidle informasjon i en slik grad som er nødvendig for å oppnå de mål som er beskrevet. Vil EOS-regelverket gi tilstrekkelig rom for "åpenhet" i samhandlingen med så vel offentlige som private aktører? Og, hvordan vil grensegangen og senteres prioritering opp mot Felles cyber koordineringssenter (FCKS) sitt virkeområde være? Kripos støtter derfor utvalgets merknader på side 86 omkring behovet for å vurdere det rettslige rammeverket knyttet til informasjonsdeling, særlig med tanke på å fjerne unødvendige hindringer for dette.

Med utgangspunkt i den grunnleggende misforståelsen som utvalget synes å ha bygget på hva gjelder politiets ansvar og oppgaver, fremstår det noe uklart for Kripos hva utvalget mener når de i kapittel 17 viser til at flere andre land de siste årene har etablert egne IKT-sikkerhetssentre og at man bør opprette et tilsvarende senter i Norge. Under kapitel 17.1 om "Oppgaver og innretning" er det blant annet vist til at man f.eks. i Storbritannia har samlet myndighetenes råd og veiledning på ett sted. Kripos vil i prinsippet kunne støtte en slik organisering, men da må Norge også følge Storbritannias eksempel fullt ut og etablere et senter med en tydelig politiprofil.

I punkt 17.2 om "Behovs- og kostnadsanalyse" er også utvalget inne på tilstøtende problemstillinger og stiller spørsmål ved om det planlagte "NSMs cybersikkerhetssenter" vil kunne favne bredt nok til å ivareta de oppgavene som et IKT-sikkerhetssenter bør ha, og å huse de eksterne deltakerne som bør være med i senteret. Kripos deler denne bekymringen og anser at oppgavene til NSMs foreslåtte cybersikkerhetssenteret i det vesentlige samsvarer med de oppgavene NSM allerede har i dag. Følgelig vil ikke denne etableringen bidra med noe vesentlig nytt i innsatsen for økt IKT-sikkerhet.

Utvalget har i kapittel 8 og 9 henvist til at det kan være enkelte styringsutfordringer knyttet til det å utvikle et IKT-sikkerhetssenter som er organisert som en del av NSM. Kripos har ikke kunnet gå grundig inn i en slik analyse, men støtter utvalget i at det er viktig at

myndighetsforankringen, herunder eventuelle styringsutfordringer mht. IKT-sikkerhetssenteret drøftes og avklares i behovsanalysen.

Forslag om ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Kripos mener i utgangspunktet at en ny lov om IKT-sikkerhet er hensiktsmessig. Særskilt støtter Kripos forslaget om rapporteringsplikt. NSRs Mørketallsundersøkelse 2018 viser til en betydelig økning av digitalt rettede ondsinnede hendelser siste to år. Mange av hendelsene burde vært rapportert til myndighetene, herunder lovbrudd anmeldt til politiet.

Hendelse defineres[1] i NIS-direktivet som "ethvert tilfelle av reell negativ virkning på sikkerheten i nettverk og informasjonssystemer". Det er verdt å merke seg at en slik ondsinnet handling kan være et forløp til en annen kriminell intensjon som kan ha større konsekvenser enn svekket IKT-sikkerhet i seg selv.

Politiet skal avverge og etterforske alle typer kriminelle handlinger. Med dagens erkjente underrapportering av uønskede digitale hendelser har ikke politiet et godt nok grunnlag for å forstå omfang og type kriminelle handlinger som skjer i det digitale rom. Økt rapportering gir bedre kunnskap. Kripos stiller seg derfor positiv til en ny lov som setter krav til at virksomheter skal varsle uønskede digitale hendelser. Hensikten med varsling/rapportering som det beskrives av Holte-utvalget, er at virksomheten som varsler skal kunne få bistand til å håndtere hendelsen.

Mulig straffeforfølgelse må inngå i håndteringsbegrepet. Det betinger at virksomheter påminnes om at en hendelse kan være ulovlig og derfor også skal rapporteres med tanke på en mulig anmeldelse med påfølgende etterforskning. Kompetent myndighet som (etter NIS direktivet) skal gi retningslinjer om når og på hvilken måte varsling skal skje, bør bidra til at anmeldelse inngår blant vurderinger som må tas. Som en del av responsmiljøenes hendelseshåndtering vil det å overrekke politiet tekniske data som mulig bevisgrunnlag være selvsagt.

Utover rapporteringskrav til virksomheter, vil en mer regulert IKT-sikkerhet gjennom lovpålegg, rammeverk og effektive styringssystemer bidra til å redusere digitale sårbarheter og gjøre dem i bedre stand til å detektere digitale angrep. Med det vil kriminelle handlinger kunne forebygges eller avdekkes raskere. Sistnevnte bidrar til at politiet kan ha et bedre teknisk datagrunnlag for sin etterforskning.

For Kripos, som selv er en *samfunnskritisk virksomhet*, vil en selvstendig IKT-sikkerhetslov kunne gi entydige sikkerhetskrav for IKT-systemer som Kripos er ansvarlig for. Føringer fra lover som Kripos allerede er underlagt hva gjelder IKT-sikkerhet oppfattes å være for lite konkrete, ikke harmoniserte og med det mer krevende å etterleve.

De resterende hovedanbefalingene fra NOU 2018:14 stiller Kripos seg bak uten å ha utfyllende kommentarer til.

[1] Art. 4(7)

SAK 2 - NIS-DIREKTIVET

Politidirektoratet ber om innspill på departementets fem konkrete spørsmål tilhørende lovutkastet til ny NIS-lov.

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

Det er fra Justis- og beredskapsdepartementet (2009) stilt krav om å følge ISO 27001/27002, herunder standardens IKT-rettede sikkerhetstiltak. Dette følger Kripos i sitt styringssystem for informasjonssikkerhet, som er en del av virksomhetens internkontroll. ITIL-prosesser inngår i den operative driften av egne IKT-tjenester.

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

Kripos har etter politiregisterforskriften et behandlingsansvar for nasjonale politiregistre. Dette innebærer blant annet kontroll/revisjon av virksomheter som i samme forskrift beskrives som databehandlere eller leverandører. Utover det at systematiske og (i større grad) enhetlige funksjonelle sikkerhetsføringer fra NIS-direktivet bidrar til bedre sikkerhet hos virksomheter den vil være gjeldende for, vil også kontroll/revisjon innenfor det mer tekniske området (nettverk- og informasjonssystemsikkerhet) kunne utøves på en mer systematisk og effektiv måte.

For andre virksomheter som NIS-direktivet vil gjelde for og som Kripos i det daglige må ha en tillit til, eksempelvis et etablert samarbeid som innebærer utveksling av beskyttelsesverdig informasjon, er det fra Kripos ståsted fordelaktig at disse underlegges strengere IKT-rettede og organisatoriske sikkerhetskrav enn de er i dag. Videre er det positivt at også disse virksomhetene pålegges rapporteringskrav om hendelser, da konsekvensen av en uønsket hendelse hos en samarbeidende virksomhet kan gi negativ ringvirkninger hos politiet og/eller hos en utenlandsk part politiet samarbeider med[2].

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

Forslagets § 10 beskriver krav om varsling for tilbydere av digitale tjenester. Her fremkommer det i 3. avsnitt at

> *"Plikten til å varsle en hendelse gjelder bare dersom tilbyderen har tilgang til informasjon som er nødvendig for å kunne vurdere om hendelsen har betydelig innvirkning på tjenesteleveransen."*

Begrepet tjenesteleveranse kan her tolkes som virksomhetens egen grunnleveranse. For politiets del kan en tjenesteleveranse i så måte være data fra en telekommunikasjonstilbyder som legger til rette for at politiet skal kunne gjennomføre kommunikasjonskontroll. I så måte

---

[2] Ref. forslagets ordlyd i § 10 om at "varselet skal inneholde nok opplysninger til at tilsynsmyndigheten eller responsmiljøet kan fastslå om hendelsen har virkninger utover Norges grenser."

er det en negativ konsekvens for politiet om ordlyden kan tolkes for snevert av den enkelte virksomhet og dermed også rapporteringsplikten.

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?

Kripos forvalter ulik type informasjon med lovpålagte krav sikkerhet og varsling. Kripos plikter at sikkerhetskrav, herunder IKT-sikkerhet, etterleves basert på krav fra blant annet følgende lover, forskrifter og instrukser:

- Politiregisterloven m/ forskrifter
- Personopplysningsloven
- Sikkerhetsloven
- Beskyttelsesinstruksen
- Lov om Schengen informasjonssystem (SIS-loven)
- Ekomloven
- eSignaturloven
- eForvaltningsforskriften
- Offentlighetsloven
- Forvaltningsloven

I Kripos' samarbeid med utlandet (blant annet Interpol, Europol og Frontex) er det inngått avtaler som setter krav til politiets IKT-sikkerhet for å påse en trygg nasjonal håndtering av informasjon som mottas fra andre land og organisasjoner.

Riksadvokatens rundskriv vedrørende kommunikasjonskontroll gir sikkerhetsføringer for hvordan slik type informasjon skal behandles.

Kripos møter Kommunal og moderniseringsdepartementets Handlingsplan for informasjonssikkerhet i statsforvaltningen (2015-2017) gjennom utledede føringer for egen sektor fra Justis- og beredskapsdepartementet.

For øvrig forholder Kripos seg til offentlig tilgjengelige veiledere og lignende fra blant annet NSM, DSB, Difi, nasjonale strategier samt etatsføringer utgitt av Politidirektoratet.

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

Kripos stiller seg positiv til en harmonisering av norsk lovverk opp mot en EØS-basert regulering med hensikt økt samfunnssikkerhet. For Kripos kan dette også bidra til en fortsatt god tillit hos utenlandske samarbeidende aktører samt en enklere etablering og etterlevelse av avtaler hvor nasjonale sikkerhetskrav inngår.

Med hilsen

Vigleik Antun
ass. sjef Kripos