Difi
Direktoratet for forvaltning og ikt

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 Oslo

Vår dato	21.3.2019
Vår referanse	19/00008-3

Deres dato	21.12.2018
Deres referanse	18/6579

Saksbehandler: Remi Longva

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

Innledning

Det er svært positivt at informasjonssikkerhet og IKT-sikkerhet blir trukket fram som et viktig politikkområde, og at regjeringen valgte å nedsette et utvalg til å utrede en del sentrale problemstillinger knyttet til disse temaene.

Vi er enige i at vi står overfor en rekke utfordringer, og støtter deler av forslagene utvalget presenterer. I dette høringssvaret konsentrerer vi oss om å utdype en del områder med våre vurderinger, og peke på behov som bør ivaretas i videre arbeid.

Høringssvaret er utarbeidet av kompetansemiljøet for informasjonssikkerhet i staten og statens kompetansemiljø for offentlige anskaffelser. Merknadene er primært begrunnet i offentlig forvaltnings behov; synspunktene kan likevel være aktuelle også for privat sektor.

Først kommenterer vi på noen sentrale problemstillinger fra NOU 2018:14 (del I-III). Deretter går vi gjennom forslagene i høringen, dvs. NIS-lovutkastet og de fem forslagene fra utvalget (NOU-ens del IV).

Generell merknad – sikkerhetsarbeidet må være helhetlig, risikobasert og ledelsesforankret

Utvalgets overordnede prinsipper

De tre overordnede prinsippene utvalget legger til grunn for sine anbefalinger synes vi er gode (NOU side 67). Hva som er tilstrekkelig sikkerhetsnivå vil variere, og IKT-sikkerhetsarbeidet må ha en risikobasert tilnærming, med fleksibel innretning.

Avveiingene som skal gjøres må baseres på en god forståelse av risiko, og av hvilke hensyn som skal ivaretas. Det finnes flere alternativer for å håndtere risiko som er av en slik betydning at den må håndteres, hvor et alternativ er å akseptere risiko. Oppgaver kan ikke løses, og tjenester kan ikke leveres, uten risiko. Da ville samfunnet stoppe opp.

Informasjonssikkerhet er ett av flere områder virksomhetene skal styre risiko på. Den siste tids debatt fra helsesektoren er i så måte illustrerende: hvor ressursbruk for primær

måloppnåelse (pasientbehandling) skal ses i sammenheng med personvern. Sikkerhetsbrudd kan få konsekvenser både for pasientbehandlingen og pasientenes andre rettigheter.

Formålet med informasjonssikkerhet er å understøtte primære målsetninger, og IKT-sikkerhet er ikke et grunnleggende mål i seg selv.

Målkonflikter

Utvalget peker på at det kan være mål- og insentivkonflikter mellom investering i sikkerhetstiltak og andre behov og ressursprioriteringer (NOU kap. 11). God forståelse av risiko, og hvilke forhold som skal avveies i beslutninger, er derfor viktig.

Utvalget trekker spesielt fram konflikt mellom effektivisering og digitalisering på den ene siden, og behovet for tilstrekkelig sikkerhet på den andre (NOU side 57 og 97). Denne konflikten kan slå uheldig ut i begge retninger:

- Digitalisering uten tilstrekkelig styring av risiko kan føre til dårlig sikkerhet
- For sterkt fokus på beskyttelse og konfidensialitetsbehov kan bremse nødvendig effektivisering

Det er tett knytning mellom målsetninger om digitalisering, effektiv forvaltning og arbeidet med informasjonssikkerhet. God informasjonssikkerhet er en forutsetning for å lykkes med digitalisering, og må inngå i et helhetlig arbeid i offentlige virksomheter[1]. For å lykkes med dette er det behov for kunnskap og god forståelse av risiko, slik at man tar gode beslutninger.

Risikobasert

Informasjonsbehandling og bruk av IKT inngår nå i stort sett all oppgaveløsning, derfor må fokuset endres fra sikkerhet i IKT-systemer og nettverk til styring av risikoen for de aktivitetene som er avhengige av de digitale miljøene.

Denne trenden synliggjøres bl.a. av dreiningen OECD tok i 2015 med sine retningslinjer for «digital risikostyring»[2]. Anbefalingen vektlegger ledelsens ansvar og involvering, og understreker behovet for risikoforståelse og kompetanse.

---

[1] Styringsaktivitetene på informasjonssikkerhetsområdet har mye til felles med de aktivitetene for styring og kontroll det er behov for på andre områder, som f.eks. personvern, HMS, kvalitet og etterlevelse av sikkerhetsloven.

[2] «the focus of the Principles has been reoriented from the “security of information systems and networks” to the security risk to the economic and social activities relying on the digital environment. [..] leaders and decision makers ultimately responsible for carrying out an activity are the best placed to set the acceptable level of risk to this activity and ensure that the digital security measures are appropriate to and commensurate with the risk, and do not undermine the activity they aim to protect. [also] need for co-operation with experts in charge of designing and maintaining the digital environment [..] who are likely to better understand the digital security risk factors and related possible security measures.” OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, https://doi.org/10.1787/9789264245471-en

Som det fremgår av mandatforståelsen har utvalgets oppdrag vært avgrenset til «IKT-sikkerhet» (NOU kap. 2.2). I dette høringssvaret vil vi ta en bredere tilnærming for å sette IKT-sikkerhet i et helhetlig risikostyringssperspektiv.

Sikkerhetsbrudd i en IKT-komponent eller et IKT-system kan få konsekvenser for informasjonssystemet de inngår i. Dette kan få konsekvenser for oppgaver og tjenester som det benyttes til, og understøtter. Det kan videre få konsekvenser utenfor virksomheten – for innbyggere, andre virksomheter og samfunnet for øvrig. Det er i konsekvensene for oppgaver og tjenester, virksomhetens mål og resultater, og for innbyggere, andre virksomheter og samfunnet for øvrig at risikoforståelsen ligger.

Virksomhetene må ivareta både egne interesser og eksterne interesser, og rammebetingelsene for virksomhetenes arbeid må ha gode føringer for hvordan risiko skal forstås og vurderes[3].

Dette betyr ikke at sikkerhet i IKT-systemer og nettverk ikke er viktig – snarere tvert imot; det er fordi det er viktig at arbeidet med dette må inngå i et helhetlig arbeid i virksomhetene, slik at ansvar for beslutninger om risiko, prioriteringer og ressursbruk ivaretas av de som har ansvaret for aktivitetene som understøttes av IKT.

Arbeidet med informasjonssikkerhet foregår primært i virksomhetene. Nasjonal sikkerhet oppnås ved at de jobber godt med dette – både for å ivareta egne interesser og eksterne interesser. I kombinasjon med myndighetenes arbeid bygger det robusthet i samfunnet – og bidrar til god samfunnssikkerhet.

Ledelse

En risikobasert tilnærming krever både ledelsesforankring og kompetanse.

Det er bred enighet om at risikoeierskapet, ansvaret for å styre risiko, må ligge hos de som har ansvaret for virksomhetens mål og resultater. Det handler om å ta beslutninger og prioritere ressursene for å nå virksomhetens mål og ivareta forskjellige interesser. Det betyr i praksis at toppledelsen etablerer og følger opp et system av styringsaktiviteter. Disse aktivitetene vil normalt gjennomføres rundt omkring i virksomheten, hvor ledere har ansvaret innen sine respektive områder.

De som har ansvaret for IKT-systemer, som både har kunnskap om hvilke hendelser som kan inntreffe og effektive sikkerhetstiltak, stiller med viktig kunnskap inn i vurdering og håndtering av risiko. Deres primære rolle er likevel som tilbydere og forvaltere av sikkerhetstiltak[4].

---

[3] Jf. eksempelvis føringer for vurdering og håndtering av risiko i NIST SP 800-37:

- consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation
- protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation

[4] Jf. «tiltaksleverandører» i Difi IK og «common control providers» hos NIST.

Dette er tilnærmingen som kommer til syne i OECDs veiledning, og som også ligger til grunn i Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»[5] (heretter kalt «Difi IK»).

Kompetanse – behov og utfordringer

Måten informasjonsbehandling og bruk av IKT inngår i all oppgaveløsning, og bygges inn i alle typer tjenesteleveranser og infrastruktur, medfører kompleksitet. Utvalget utreder dette på en god måte. Det handler om å innse at vi beveger oss inn i fremtiden med ny og ukjent risiko – og være motivert for å forsøke å forstå den, og ha tilstrekkelig styring av den, for å være i stand til å løse oppgaver og levere tjenester på en god måte. Dette er selvfølgelig krevende – som så mange andre områder av samfunnet og ledelse av en virksomhet er det.

Norsk regelverk er i stor grad funksjonsbasert. Det vil si at det stiller krav til hva som skal oppnås, men er fleksibelt med tanke på de spesifikke detaljene i hvordan det skal oppnås. Det er stort rom for tilpasning til en virksomhets størrelse, egenart og risiko. Slik fleksibilitet er positivt, ettersom det gjør det mulig å tilpasse styringsaktiviteter og sikkerhetstiltak til lokale behov, og sørge for at sikkerhetsarbeidet både er formålseffektivt og kostnadseffektivt.

Ulempen er at det kan være kompetansekrevende. Det krever kompetanse i ledelse, organisering og innen endringsstyring kulturutvikling. Det krever evne til å gjøre gode vurderinger av, og ta beslutninger om, risiko. Det krever tilstrekkelig faglig kunnskap til å velge, etablere og forvalte hensiktsmessige sikkerhetstiltak – samt fase ut sikkerhetstiltak som ikke lenger er nyttige.

I internasjonal målestokk har Norge hovedsakelig små virksomheter, og for mange av disse er det en utfordring å dekke alle behovene innen virksomhetsstyring, inkludert informasjonssikkerhet.

Virksomheter som legger lite vekt på styringsaktiviteter, men i stedet hovedsakelig går inn for etablering av anbefalte sikkerhetstiltak fra en tiltaksbank, vil også kunne oppleve utfordringer med kompetanse. Kompetanse- og ressursbehovet kan være stort for å etablere og forvalte sikkerhetstiltak. De vil i tillegg ende opp med utfordringene som følger av utilstrekkelig ledelsesforankring og svak styring.

Det er svært viktig at myndighetenes videre arbeid innen informasjonssikkerhet legger vekt på å heve kompetanse[6]. Det er behov for kompetanse på mange områder, og både i departementene og i virksomhetene.

Som utvalget påpeker, så kan kompetansebehovet også avhjelpes med andre virkemidler; god regulering og tilhørende anbefalinger og veiledning.

Verdikjedeproblemet

I NOU kap. 3.2 skriver utvalget om verdikjeder: «på grunn av de digitale verdikjedene er det ingen virksomheter som har full oversikt over egne sårbarheter.»

---

[5] https://internkontroll-infosikkerhet.difi.no/

[6] Jf. nasjonal strategi for digital sikkerhetskompetanse, https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

Vi vil anta at det vil være behov for å gå opp grenseganger i ansvarsforhold, organisatorisk og teknologisk; hvem som har råderett over hva. Det kan være fornuftig å ta utgangspunkt i informasjonssystemer, inkludert system-av-systemer («infrastruktur»). En av problemstillingene er hva som skal være førende for beslutninger om risiko, og hvilke mekanismer man skal bruke for å ivareta tilstrekkelig sikkerhetsnivå for ulike behov.

Selv om håndtering av verdikjeder blir utredet senere, så har problematikken knytning til reguleringen som utvalget har blitt bedt om å se på. Disse sammenhengene, og hvordan forslag til regulering bidrar til å løse disse utfordringene bør inngå i videre arbeid.

Systemutvikling

Etter vårt syn er det viktig at informasjonssikkerhet designes og bygges inn i informasjonssystemer og tekniske løsninger. Vi savner nærmere omtale av systemutvikling, inkludert programvareutvikling, i NOU-en.

Forslagene i høringen

Lov om sikkerhet i nettverk og informasjonssystemer (NIS-loven)

Lovutkastet skal gjennomføre NIS-direktivet. Direktivet setter krav til et passende sikkerhetsnivå for tilbydere av samfunnsviktige tjenester og digitale tjenester, og gir førstnevnte gruppe også noen varslingsplikter. Det gjennomgående kravet er at hensiktsmessige og rimelige tekniske og organisatoriske tiltak iverksettes, slik at sikkerhetsnivået står i forhold til risikoen.

Dette kravet er i det vesentlige i tråd med gjeldende rett, jf. gjennomgangen i høringsnotatets kapittel 7.1, selv om uttrykksmåtene varierer og at dagens lovbestemmelser på noen områder kan ha en uklar rekkevidde når det gjelder sikring av IKT-systemer.

NIS-lovens krav til sikkerhetsnivå synes altså i liten grad å kreve tilpasninger i virksomhetene.[7] Difi ser imidlertid at det kan være pedagogiske fordeler med en lovfesting av kravet til risikostyring i virksomheten (ev. begrenset til en del av virksomheten, IKT-sikkerhet, informasjonssikkerhet, IKT-tjenester), og at tjenestene som dekkes av loven skal ha et særlig fokus på kontinuitetssikring (mao. et særlig tilgjengelighets-/integritetsfokus).

Når det gjelder fremstillingen av eforvaltningsforskriften § 15 vil vi presisere at bestemmelsen forutsetter etablering av sikkerhetstiltak, inkludert organisatoriske og tekniske tiltak. Forskriften peker ikke på hvilke tiltak som skal gjennomføres, men å ha «internkontroll [..] på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet»[8] innebærer krav om tilstrekkelig håndtering av risiko, som inkluderer tilstrekkelige sikkerhetstiltak. Kravet i bestemmelsen kan ikke etterleves i praksis uten at sikkerhetstiltak etableres og forvaltes.

---

[7] Dette stemmer også med analysen fra EU for våre nordiske naboer, jf. at kostnadene ved implementering av NIS-direktivet er beregnet for å heve sikkerhetsnivået hos de svakeste aktørene; Nordens EU-medlemmer er klassifisert i øverste klasse, som «the champions», jf. SWD(2013) 32 finalv, kapittel 4.2.1.

[8] Difi er utpekt til å gi anbefalinger på området, og virksomhetene anbefales å basere seg på ISO/IEC 27001:2013. Difi IK tilbyr praktisk veiledning basert på denne standarden, inkludert en prosessmodell med beskrivelse av de styringsaktivitetene en virksomhet vil ha behov for.

For å sikre sammenheng med øvrig virksomhetsstyring anbefaler vi at NIS-loven inkluderer en bestemmelse om at risikostyringen skal inngå i helhetlig styring og kontroll. Vi vil da anbefale at man gjenbruker formuleringer fra eforvaltningsforskriften § 15, f.eks. ved å ta inn følgende setning i § 7 nytt fjerde ledd, eventuelt også i § 9 nytt fjerde ledd:

- Risikostyringen på IKT-sikkerhetsområdet bør være en integrert del av en helhetlig internkontroll. Omfang og innretning på internkontrollen skal være tilpasset risiko.

Et slikt tillegg vil klargjøre at risikostyring innen NIS-lovens område bør knyttes til øvrig risikostyring i virksomheten. Dette vil sikre samsvar med annet regelverk og anbefaling i internasjonale standarder. Dersom ordensforskrifter ikke ønskes i bestemmelsen, kan man oppnå noe av det samme ved å føye til bestemmelsen at arbeidet skal være risikobasert og systematisk. Det er gjort i den svenske loven.[9]

De pedagogiske fordeler ved lovregulering kan imidlertid tapes dersom rettsanvenderne opplever at NIS-lovens metodekrav bryter med krav i andre særlover/-forskrifter, eller introduserer usikkerhet med hensyn til hvordan risikostyringen skal gjennomføres. I lys av dette vil vi anbefale

- at formålsbestemmelsen (§ 1) eller tiltakspliktsbestemmelsene (§§ 7 og 11) tydelig peker på at lovens hovedfokus er å sikre kontinuitet i tjenester, slik at risikoen for manglende kontinuitet må vurderes. Vi tror et slikt tillegg vil være til hjelp for forståelsen av hva dette regelverket særlig søker å oppnå.
- at tiltakspliktsbestemmelsene i §§ 7 og 9 søkes harmonisert med personvernforordningens artikkel 32[10] når det gjelder momenter som skal hensyntas, og ikke begrenser seg til å peke på «teknisk utvikling». Som departementet peker på vil praktisk talt alle virksomheter måtte skaffe seg kompetanse på vurdering av risiko iht. personvernforordningens krav (jf. høringsnotatet side 40-41). Hvis bestemmelsen legger svært ulike føringer for vurderingene, blir regelverket mer komplekst, og potensielt mindre effektivt.

Lovforslaget legger opp til at man i forskrift kan gi mer detaljerte sikkerhetskrav, inkludert krav til sikkerhetstiltak, organisatoriske eller tekniske. For digitale tjenester synes direktivets artikkel 16 nr 10 å sette begrensninger på hvordan en slik hjemmel kan utnyttes, men vi finner ikke grunn til å gå nærmere inn på en slik regulering, jf. at eventuelle krav vil bli sendt på høring.

Vi vil imidlertid understreke behovet for at eventuelle mer detaljerte krav begrunnes i gode vurderinger, hvor både tiltakets risikoreduserende effekt og potensielle negative sideeffekter hensyntas. Praksis knyttet til varslingsplikten i loven vil kunne gi innsikt i sikkerhetsutfordringer som virksomhetene ikke er tilstrekkelig oppmerksom på, og som

---

[9] «11 § Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.»

[10] Artikkel 32 nr 1 «1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter»

eventuelt kan møtes med egnede tiltak, enten de er regulatoriske, kompetanserettede eller annet.

Direktivet etablerer en krevende arbeidsdeling mellom ulike regelverk når det gjelder varsling, som vil kunne gi vanskelige tolkningsspørsmål. Tillitstjenestelovens varslingsregler vil ha forrang foran NIS-direktivets varslingsregler. Samfunnsviktige tjenester må derfor vurdere om de også vil regnes som tillitstjenester iht. eIDAS artikkel 3 nr 16[11]. For Difis egen virksomhet vil det blant annet være et spørsmål om løsningen for autentisert signatur skal regnes som en tillitstjeneste – den tilbyr forseglede bevis for innlogginger, som nok kan være dekket av ordlyden i 3 art 16 bokstav c.

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

Utvalget foreslår at NIS-lovutkastet gis et utvidet virkeområde, ved at loven også skal gjelde all offentlig forvaltning.

Vi er enig med utvalget når de skriver at «Når det gjelder konsekvensene av å innlemme hele offentlige forvaltning i den nye loven er det flere usikkerhetsfaktorer.» (NOU side 71)

Utvalget foreslår at det opprettes et lovutvalg (NOU kap. 15.7). Vi mener det er behov for et slikt utvalg før det innføres ny regulering som skal gjelde all offentlig forvaltning. Vi vil i den anledning peke på flere områder som det bør ses nærmere på. Våre vurderinger avviker noe fra NOU-ens antakelser om hvordan en slik lov bør innrettes. Vi peker blant annet på flere muligheter for å øke verdien på ny regulering.

Virkeområde og innretning

Regelverk for informasjonssikkerhet bør være funksjonsbasert, risikobasert og legge til rette for tilpasning i virksomhetene. Vi oppfatter det slik at utvalget deler vårt syn på dette. Den nye personvernforordningen og den nye sikkerhetsloven er eksempler på regulering som er basert på dette prinsippet.

Formålet med informasjonssikkerhet er å understøtte andre målsetninger. Hva som skal være førende for vurderingene virksomhetene skal gjøre av risiko, inkludert hvilke interesser som skal ivaretas, mao. hvilke konsekvenser som skal unngås, bør fremstå tydelig.

Et generelt krav om tilstrekkelig informasjonssikkerhet, inkludert IKT-sikkerhet, i forvaltningen bør legges i lov. Områder som har særlige behov bør skilles ut, slik at man kan gi særlige regler for disse områdene. Så langt det overhode er mulig bør man likevel gjenbruke terminologi og vise til overordnet regelverk. Et eksempel er sikkerhetsloven; den gir en rekke særregler, men tar utgangspunkt i styring og kontroll i en helhetlig tilnærming i virksomhetene.

Det er flere områder som krav i en eventuell ny regulering kan rette seg mot, blant annet:

- styringsaktiviteter
- overordnete føringer for sikkerhetsnivå

[11] Merk at det er intet krav om at tjenesten er kvalifisert tillitstjeneste.

- overordnede minimumskrav til sikkerhetstiltak
- spesifikke sikkerhetstiltak som skal etableres og forvaltes

Regulering av styringsaktiviteter

Forvaltningen har i dag en rekke regler som stiller krav til tilstrekkelig og risikobasert styring og kontroll generelt[12] og innen spesifikke områder[13].

Det bør være tydelige krav om at virksomhetene plikter å ha tilstrekkelig styring og kontroll, og styre risiko tilknyttet informasjonsbehandlingen som en del av helhetlig ledelse og styring av virksomheten. Dette antas blant annet å ha en pedagogisk effekt. Dette danner grunnlaget for øvrige mer detaljerte bestemmelser.

Bestemmelser som stiller krav til innholdet i styringsaktivitetene kan legges til forskrift[14]. Her bør man sørge for harmonisering med etablert og god praksis, for eksempel Difi IK, som er basert på ISO/IEC 27001.

Regulering av sikkerhetstiltak

I utgangspunktet tror vi at dersom regulering, spesielt begrepsbruk og overordnede prinsipper, er tilstrekkelig koordinert og oversiktlig, kan øvrige behov i stor grad dekkes av anbefalinger og veiledning.

En virksomhet som etablerer et sett sikkerhetstiltak uten å først kjenne egne behov kan ende opp uten nødvendig ledelsesforankring og uten tilstrekkelig forståelse av risiko og behov. For en del virksomheter kan det ende med ressursforspillelse, etterlevelse framfor tilstrekkelig sikkerhet, og at de opererer med ukjent og potensielt høy risiko.

Det at virksomhetene har problemer med å finne riktig sikkerhetsnivå kan løses på forskjellige måter; det er ikke nødvendigvis klart at å fastsette ett nivå som skal gjelde for alle vil gi et godt resultat

Dersom man skal regulere sikkerhetstiltak er det flere måter å gå frem på:

- Det kan stilles overordnede krav til sikkerhetsnivå.
- Det kan stilles overordnede minimumskrav til sikkerhetstiltak[15].
- Det kan stilles minimumskrav til spesifikke sikkerhetstiltak som virksomhetene skal etablere og forvalte, enten i form av forskriftsbestemmelser[16], eller ved å peke på en tiltaksbank som skal benyttes.

---

[12] Jf. økonomiregelverket i staten og kommuneloven.

[13] Jf. bl.a. efvf § 15, personvernforordningen for behandling av personopplysninger, arbeidsmiljøloven med internkontrollforskriften, samt sikkerhetsloven.

[14] Denne tilnærming er brukt i sikkerhetsloven og dens forskrifter.

[15] For eksempel, se FIPS 200 i USA.

[16] Sikkerhetsloven med forskrifter stiller både overordnede krav til sikkerhetsnivå og minimumskrav til spesifikke sikkerhetstiltak.

- Minimumskrav til sikkerhetstiltak kan videre deles inn i nivåer[17]; det kan for eksempel være ett sett sikkerhetstiltak som skal bidra til å sikre alle informasjonssystemer, og et utvidet sett som skal bidra til tilstrekkelig grunnleggende sikkerhet der konsekvensene ved sikkerhetsbrudd forventes å kunne bli høye, f.eks. viktige fellesløsninger i forvaltningen.

Omfang og kategorier av sikkerhetstiltak det skal stilles krav til bør vurderes nøye. Utvalget peker på NSMs grunnprinsipper for IKT-sikkerhet. Denne tiltaksbanken har begrensninger; for eksempel mangler den flere kategorier av sikkerhetstiltak som internasjonalt anerkjente tiltaksbanker inneholder; blant annet innen systemutvikling og personellsikkerhet[18].

Det er fordeler og ulemper ved alle variantene, og disse bør vurderes nøye. Vi foreslår at man også gjør vurderinger av erfaringer fra andre land, for eksempel av mekanismene som benyttes av NIST for forvaltningen i USA.

Det er uansett svært viktig at lov- og forskriftsbestemmelser ledsages av anbefalinger og veiledning, uavhengig av omfang og innretning på regulering av sikkerhetstiltak.

Vår vurdering og anbefaling

Vi er usikre på hvor stor nytte og effekt lovforslaget vil ha for offentlig forvaltning. Det er i dag en rekke regelverk som pålegger forsvarlig informasjons- og IKT-sikkerhet. En hovedutfordring for virksomhetene er å etablere effektiv styring[19], slik at de oppnår tilstrekkelig sikkerhet og ivaretar alle behov.

Ny regulering kan gi samfunnsøkonomisk nytte[20], men det er behov for å se nærmere på innretning på reguleringen; slik at den får tilstrekkelig helhetlig tilnærming, og er egnet til å danne utgangspunkt for en fremtidig harmonisering av regelverk.

Forslaget stiller blant annet ikke krav til informasjonssikkerhet for all informasjonsbehandling, men retter seg i hovedsak inn mot sikring av teknologien som benyttes. Forslaget stiller ikke tydelige krav til styring og kontroll, som en del av helhetlig styring i virksomhetene. Eventuell

---

[17] For eksempel, se bruken av «baselines» i NIST SP 800-53 i sammenheng med FIPS 199.

[18] «Første versjon av grunnprinsippene handler om teknologiske og organisatoriske tiltak for å sikre IKT-systemer. Det menneskelige perspektivet og fysisk sikkerhet vil inkluderes i senere versjoner.» NSMs Grunnprinsipper for IKT-sikkerhet, versjon 1.1.

[19] «Vår vurdering er at hver tredje statlige virksomhet ikke har tilstrekkelig styring og kontroll på informasjonssikkerheten. Det er stor variasjon på innretning og omfang på styring og kontroll i virksomhetene.» Difi-rapport 2018:4 – Arbeidet med informasjonssikkerhet i statsforvaltningen. https://www.difi.no/rapport/2018/06/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen

[20] «Spørsmålet om tiltaket er samfunnsøkonomisk lønnsomt vil avhenge i veldig stor grad av hvordan en ny lov formuleres.» (kap. 5.7) og «En «perfekt» IKT-sikkerhetslov vil utvilsomt kunne føre til bedre IKT-sikkerhet, men det er antakelig for mange usikkerhetsfaktorer til at man kan etablere en slik lov uten at det foretas ytterligere utredninger.» (kap. 5.8) i Samfunnsøkonomisk vurdering av anbefalinger fra IKT-sikkerhetsutvalget, Oslo Economics.

regulering av minimumskrav til sikkerhetstiltak kan innrettes på forskjellige måter, kan bidra til å dekke flere behov samtidig, og bør utredes nærmere.

Dersom det skal opprettes et lovutvalg, vil vi anbefale følgende:

- Mandatet bør gjelde lovforslag om informasjonssikkerhet.
    - Dette må inkludere all informasjonsbehandling, i tillegg til IKT-systemer og digitale tjenester.
- Kompetanse i lovutvalget er viktig, og juridisk-, forretnings- og digitaliseringskompetanse må inngå. Kommunal sektor bør være representert.
- I lys av tidligere undersøkelser[21] vil vi anta at kravene primært bør knyttes til styringsaktiviteter.
- Helhetlig regulering er viktig, men ambisjon for opprydning må sees i lys av kompleksiteten i eksisterende regelverk.
- Omfang av og innretning på krav til sikkerhetstiltak bør vurderes nøye.
    - Det må tas hensyn til kost-nytte; hvor ønsket effekt, kostnader og potensielle negative sideeffekter inngår.
    - Man bør vurdere eventuell nytte et felles sett med sikkerhetstiltak (tiltaksbank) for offentlig sektor kan ha i forbindelse med anskaffelser, inkludert forslag om markedsplass for skytjenester.
    - Man bør vurdere om det er behov for inndeling i nivåer, og hvilken innretning det eventuelt bør ha.
    - Sammenheng med andre virkemidler, spesielt anbefalinger og veiledning.
    - Man bør vurdere eventuell nytteeffekt et felles sett med sikkerhetstiltak (tiltaksbank) kan ha for kunnskaps- og erfaringsutveksling mellom virksomheter, uavhengig av om det er krav, anbefalinger eller en kombinasjon av disse.

Det bør vurderes om en del krav og anbefalinger er hensiktsmessig å legge til andre normerende dokumenter, eksempelvis referansekatalogen for offentlig sektor[22]. For sistnevnte er det på informasjonssikkerhetsområdet gitt noen anbefalinger og krav, basert på vurderinger av kost-nytte og med involvering av relevante parter[23].

---

[21] Styringssystem for informasjonssikkerhet. Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002. Rapport 2012:15 ISSN 1890-6583. https://www.difi.no/rapport/2014/03/styringssystem-informasjonssikkerhet-erfaringer-med-og-anbefalinger-om-standardene

[22] https://www.difi.no/referansekatalogen

[23] https://www.difi.no/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet

Krav om IKT-sikkerhet ved anskaffelser

Difi vektlegger informasjonssikkerhet og IKT-sikkerhet i vårt arbeid med offentlige anskaffelser.

IKT-sikkerhet i offentlige anskaffelser

Anskaffelsesregelverket er et generelt regelverk som setter prosesskrav mv. til alle typer anskaffelser. Andre regelverk inneholder en rekke særregler som stiller krav som må hensyntas i anskaffelsen, for eksempel krav til bygg, kjøretøy mv. Dersom man skal inkludere særkrav i anskaffelsesregelverket, kan regelverket bli svært omfattende og detaljert.

Alle offentlige virksomheter er pålagt å styre risiko knyttet til sine oppgaver og tjenester, dette gjelder også når disse understøttes ved bruk av anskaffelser, herunder tjenestekjøp.

Vi legger til grunn at utvalgets forslag gjelder anskaffelser som involverer IKT-tjenester. I tilfeller hvor IKT-tjenester inngår som en del av tjenesten som anskaffes, f.eks. ved at en leverandør av forbruksmateriell er knyttet til kundens lagerstyringssystem, må kunden stille krav til tilstrekkelig IKT-sikkerhet. Ved anskaffelse av tjenester som hverken direkte eller indirekte omfatter informasjonsbehandling eller IKT-tjenester er det lite relevant å stille krav om IKT-sikkerhet. Det er viktig å ta hensyn til kravet om «forholdsmessighet» når det skal vurderes hvilke krav som skal stilles, slik at det ikke hemmer konkurransen og fordyrer tjenestene.

Hva det skal stilles krav til i anskaffelser

Utvalget mener det skal stilles tydeligere krav til IKT-sikkerhet ved anskaffelser, men peker i liten grad hva dette innebærer, utover at kravene skal gi «forsvarlig IKT-sikkerhet».

Det kan for eksempel stilles krav til:

- Styringsaktiviteter hos leverandør
- Samhandling i styringsaktiviteter mellom kunde og leverandør
    - F.eks. knyttet til vurdering av risiko eller håndtering av hendelser
- Innsyn i dokumentasjon som produseres av styringsaktivitetene hos leverandør
    - F.eks. føringene som gjelder hos leverandøren og hvordan disse følges opp, inkludert resultater fra virksomhetsledelsens gjennomgang, eller informasjon om ytelse på sikkerhetstiltak og oppfølging av hendelser
- Overordnede krav til sikkerhetsnivå
    - F.eks. kategorier av sikkerhetstiltak og omfang og styrke på disse
- Krav om spesifikke sikkerhetstiltak
- Krav om tillitsinformasjon
    - Sertifiseringer
    - Rapporter attestert av tredjeparter (f.eks. SOC 2)

Samordning av kravstilling fra offentlig sektor til leverandørmarkedet

Det fremstår som uklart i hvilken grad utvalget mener det er behov større grad av felles krav til informasjonssikkerhet i anskaffelser, uavhengig av virksomhetenes egne vurderinger, eller hvordan utvalget mener dette bør innrettes.

Det er flere problemstillinger som er aktuelle å se nærmere på i det videre arbeidet på området, for eksempel:

- Nytten av større grad av samkjørt kravstilling fra offentlige virksomheter til leverandørmarkedet – inkludert potensiell effektiviseringsgevinst for begge parter.
- Nytten av felles tiltaksbank for offentlig sektor også i forbindelse med anskaffelser og forslag om markedsplass for skytjenester[24].
- Hvilke muligheter Norge har for nasjonale særkrav i et internasjonalt marked som for en god del tjenester forventes å være dominert av internasjonale giganter.
- Hvilken nytte Norge har av å samordne nasjonale krav mot internasjonale krav og tiltaksbanker, som den nevnte typen leverandører pr i dag som regel har ivaretatt i sine tjenester.

I statens standardavtaler (SSA) er det stilt krav til informasjonssikkerhet, for eksempel i SSA-D kap 1.1 artikkel 9.2. Difi har startet et arbeid med å revidere SSA-ene. I dette arbeidet vil behov for ytterligere krav til informasjonssikkerhet bli vurdert.

Styrking av sikkerhet i tilknytning til anskaffelsesregelverket må balanseres mot behovet for innovative og digitale anskaffelser.

Hvor kravene skal komme fra

Utvalget skriver at «Det må gjøres konkrete vurderinger av krav om sikkerhet ved hver anskaffelse, og de relevante kravene må beskrives i kravspesifikasjonene og bilagene til avtalen.» (NOU kap. 16.1.)

Dagens regulering er hovedsakelig funksjonsbasert, og virksomhetene har selv ansvaret for å vurdere behov for informasjonssikkerhet i sine oppgaver og tjenester. Det er få bestemmelser om spesifikke sikkerhetstiltak[25].

Utvalget foreslår ny regulering som kan inkludere at mer detaljerte krav rettes til offentlige virksomheter, inkludert krav om spesifikke sikkerhetstiltak. Hele eller deler av disse kravene må nødvendigvis videreføres som krav til leverandører av tjenester som innebærer informasjonsbehandling, inkludert IKT-tjenester.

Vi anbefaler at offentlige virksomheters behov for å håndtere krav til sikkerhet i anskaffelser ses i sammenheng med videre arbeid med ny regulering.

Et nasjonalt IKT-sikkerhetssenter

Det er nytte å hente i styrket offentlig-privat samarbeid, inkludert kompetanseutvikling og styrket koordinering av hendelseshåndtering.

Det er behov for et godt tilbud med veiledning om IKT-sårbarheter, god praksis i hendelseshåndtering og detaljerte råd og veiledning om sikkerhetstiltak: utforming, etablering og forvaltning av grupper av slike, og spisset veiledning om enkelttiltak.

---

[24] For eksempel på dette, se FedRAMP-programmet i USA.

[25] Et av unntakene er forskrifter til sikkerhetsloven. Disse er mest relevant for sikkerhetsgradert anskaffelser, som det er egne regler for.

Slik veiledning bør knyttes opp mot tiltaksbank(er), regelverksbestemmelser om spesifikke sikkerhetstiltak og aktuell risiko. Krav, anbefalinger og veiledning bør henge godt sammen, slik at det gir god nytteverdi til virksomhetene. Et IKT-sikkerhetssenter kan være spesielt godt egnet til å dekke behovet for veiledning innen flere kategorier av sikkerhetstiltak.

Det er viktig at veiledning rettet mot offentlige virksomheter henger godt sammen med veiledning på tilstøtende områder. Vi tenker blant annet på veiledning innen styring og kontroll, inkludert risikostyring, og veiledning innen ledelse, digitalisering, informasjonssikkerhet, informasjonsforvaltning og offentlige anskaffelser fra Difi og Direktoratet for økonomistyring (DFØ). Ansvarsdeling mellom nytt senter og eksisterende aktører må være tydelig.

Utvalget viser til eksempel på samordnet veiledning i form av en nettportal i Sverige (informationssakerhet.se). Den svenske portalen tar et mer helhetlig utgangspunkt i informasjonssikkerhet.

Den behovs- og kostnadsanalysen utvalget foreslår at gjennomføres bør bl.a. se nærmere på:

- Hva et slikt senter skal gi råd og veiledning om
- Hva som skal koordineres ved hjelp av et slikt senter
- Hvordan man bør gå fram for å styrke sammenhengen mellom «digital» hendelseshåndtering og beredskap og øvrig beredskapsarbeid i samfunnet

Regulering og ansvar for tilkoblede produkter og tjenester

Dette er et område hvor internasjonalt samarbeid er viktig, særlig opp mot regelverksprosesser i EU. Norge er et av de mest digitaliserte samfunnene i Europa, storforbrukere av slike produkter, og etter vårt syn bør Norge bør være aktive og sørge for fremdrift på området.

I det videre arbeidet bør det tydeliggjøres hvilken linje Norge bør legge seg på, gjerne knyttet til vurdering av innholdet i initiativene som det henvises til i NOU-en kap. 18; det britiske politikkdokumentet fra 2018 og EUs forslag til Cybersecurity Act.

Temaet er viktig og relevant også for offentlige virksomheter, ettersom de benytter slike produkter og tjenester.

Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Som nevnt innledningsvis handler informasjonssikkerhetsarbeidet om styring av ett av flere områder av operasjonell risiko i virksomhetene[26][27]. At virksomhetene har dette perspektivet bør inngå i innretningen på nasjonal styring og koordinering. Det er spesielt viktig i forbindelse med samordning av styringssignaler fra departementene, slik at risikostyring på informasjonssikkerhetsområdet inngår i virksomhetsstyringen for øvrig.

Etter vårt syn er det ikke tilstrekkelig belyst hvordan myndighetene bør gå fram for å få til den ønskede samordningen i en slik helhet. I videre arbeid blir det viktig å se på innholdet i

[26] https://dfo.no/fagomrader/internkontroll/internkontroll-i-virksomhetsstyringen

[27] https://dfo.no/fagomrader/risikostyring/sammenhengen-mellom-risikostyring-og-internkontroll

styringssignalene, inkludert hvilket detaljnivå føringer til og oppfølging av virksomhetene bør legges på.

Finansdepartementet og DFØ har ansvaret for veiledning på etatsstyring i departementene og internkontroll og risikostyring i virksomhetene. Med bakgrunn i et kunnskapsgrunnlag[28] Difi utarbeidet i 2018, blir det etablert et prosjekt som tar sikte på å forbedre etatsstyring på informasjonssikkerhetsområdet. Dette inngår i et samarbeid mellom flere statlige aktører, inkludert DFØ, Difi og Nasjonal sikkerhetsmyndighet (NSM).

Avslutning

Høringen omhandler tema av stor betydning for samfunnet. Ved å belyse flere sider ved forslagene kan effekten og samfunnsnytten økes. Tilstrekkelig vekt på styrket ledelsesforankring, og betydningen av helhetlig arbeid og risikoforståelse hos ledelsen i virksomhetene, bidrar til en formåls- og kostnadseffektiv tilnærming til informasjonssikkerhet. Det vil understøtte forskjellige målsetninger og behov i samfunnet, inkludert behov for effektiv digitalisering og nasjonal IKT-sikkerhet.

Difi arbeider sammen med andre aktører for å styrke og samordne anbefalinger og veiledning. Vi ser fram til videre samarbeid for å møte utfordringene utvalget peker på og oppnå regjeringens målsetninger på området.

Vedlegg:

1. Begreper som benyttes i høringssvaret
2. Spørsmål i høringsbrevet, Difis egen virksomhet

Vennlig hilsen
for Difi

Grete Orderud
Avdelingsdirektør

Kjetil Korslien
Fung. seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.

[28] https://www.difi.no/rapport/2018/06/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen

Kopi til:

Kommunal- og moderniseringsdepartementet	Postboks 8112 Dep	0032 OSLO

Vedlegg 1 – begreper som benyttes i høringssvaret

Denne høringen omhandler temaer hvor det benyttes mange begreper som forstås forskjellig på ulike fagområder, og det er fagområder som griper inn i hverandre. Vi gir her en kort beskrivelse av hva vi legger i noen av begrepene i dette høringssvaret.

Informasjonssystem og IKT-system[29]

Informasjon behandles i et samspill mellom mennesker, prosesser og teknologi. Når vi bruker «informasjonssystem» mener vi et avgrenset sett med ressurser som behandler informasjon – dette inkluderer mennesker, prosesser og teknologi. Vi benytter «IKT-system» eller «IKT-tjeneste» når vi mener et teknisk system av program- og maskinvare.

Tilrettelegging av arbeidsoppgaver (prosesser), slik at det er enkelt for mennesker å utføre sine oppgaver med god sikkerhet, og tiltak innen kompetanse og kultur er viktig for å sikre alle elementene i informasjonssystemet.

Informasjonssikkerhet og IKT-sikkerhet

Arbeidet med informasjonssikkerhet handler om å sikre informasjonsbehandling – i sammenheng med oppgaver og tjenester som den inngår i og understøtter.

Det betyr å sikre at informasjon i alle former[30]

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Det inkluderer å sikre informasjonssystemene som benyttes – inkludert alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i informasjonssystemene.

Styringsaktiviteter og sikkerhetstiltak

Vi skriver «styringsaktiviteter» når vi mener de sentrale aktivitetene som normalt inngår i styring og kontroll på informasjonssikkerhetsområdet. Jf. ISO/IEC 27001 (kapittel 4 til 10) og de systematiske aktivitetene som er beskrevet i Difi IK.

Vi skriver «sikkerhetstiltak» når vi mener de varige tiltakene som en virksomhet etablerer for å operere med redusert risiko tilknyttet informasjonsbehandlingen. Dette er tiltak som ved en risikobasert tilnærming velges og etableres ved bruk av styringsaktivitetene «risikovurdering» og «risikohåndtering». For en mer detaljert beskrivelse, se artikkel om sikkerhetstiltak i Difi IK[31].

---

[29] Jf. innholdet i begrepet «informasjonssystem» i sikkerhetsloven og i NIS-direktivet.

[30] Inkludert «digitale data» og data som kun benyttes maskinelt (ikke nødvendigvis ment for å leses og forstås av mennesker).

[31] https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/sikkerhetstiltak

Tiltaksbanker

Vi skriver «tiltaksbanker» når vi mener referansekataloger, eller rammeverk, med sikkerhetstiltak. For eksempel ISO/IEC 27002[32] eller NIST SP 800-53 «Security and Privacy Controls for Information Systems and Organizations», som er en katalog med sikkerhets- og personverntiltak som virksomheter i føderal forvaltning i USA må benytte. Difi IK har en artikkel med nærmere omtale av flere andre tiltaksbanker og bruken av disse[33].

I NIST SP 800-53 sorteres sikkerhetstiltakene i «familier». I nåværende utgave av ISO/IEC 27002 er de sortert etter «kategorier». I NISTs Framework for Improving Critical Infrastructure Cybersecurity («Cybersecurity Framework») er gruppering etter «funksjoner», eller formål: Identify – Protect – Detect – Respond – Recover.

NIST SP 800-53 bruker «baselines» for nivådeling, NIST CSF benytter «tiers».

[32] Referansekatalogen (Annex A) i ISO/IEC 27001 inneholder de samme sikkerhetstiltakene som er nærmere beskrevet i ISO/IEC 27002.

[33] https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/tiltaksbanker

Vedlegg 2 – Spørsmål i høringsbrevet, Difis egen virksomhet

Vi har skilt mellom den generelle omtalen av NOU-en og lovforslaget og spørsmålene som rettes til Difis egen virksomhet i høringsbrevet. Sistnevnte adresseres her av de som har fagansvar for styringen i Difi.

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

Difi gjennomfører systematiske aktiviteter for å sikre konfidensialitet, integritet og tilgjengelighet av informasjon. Ledelsens forankring, utøvelse av rolle og ansvar og risikobasert tilnærming er de aller viktigste prinsippene. Arbeidet omfatter både nasjonale fellesløsninger, andre digitale tjenester og Difis interne systemer. Styring av informasjonssikkerhet i Difi baserer seg på ISO/IEC 27001.

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

Vår foreløpige vurdering er at vi ikke forventer at det vil medføre organisatoriske og tekniske tiltak som vi ikke allerede har i dag. Vårt arbeid er allerede risikobasert, og vi stiller høye krav til sikkerhet i ID-porten, andre fellesløsninger og Difis virksomhet for øvrig.

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

Det blir et ekstra regelverk som vi må forholde oss til. Helhetlig håndtering av regelverk er en generell utfordring. F.eks. kan varslingsplikter bli mer komplekse, og de må koordineres.

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?

Difi, som et statlig forvaltningsorgan, er underlagt en rekke regelverk som stiller krav til sikkerhet. Noen av de mest aktuelle er forvaltningsloven, offentleglova, personopplysningsloven, arkivloven, sikkerhetsloven, lov om offentlige anskaffelser, samt tilhørende forskrifter. E-forvaltningsforskriften stiller krav til styring av informasjonssikkerhet. Økonomiregelverket i staten stiller overordnede krav til internkontroll, som medfører behov for sikkerhet og beredskap.