Forsvarsminister **Ine Marie Eriksen Søreide,**
Forsvardepartementet

Oslo, 20. januar 2017

Høringsinnspill fra Abelia:

NOU 2016:19 "Samhandling for sikkerhet"

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, vi har ca. 2000 medlemsbedrifter med omtrent 46.000 ansatte over hele landet. Abelia har medlemmer innenfor blant annet IKT, undervisning, forskning, konsulenttjenester, kreative virksomheter og interesseorganisasjoner. For en digital versjon av dette høringsinnspillet se her; https://www.abelia.no/samhandling-for-sikkerhet

Innledning

Abelia vil starte med å gi honnør til Regjeringen for at den i mars 2015 satte ned et uavhengig utvalg for å utrede og foreslå et nytt lovgrunnlag for forebyggende nasjonal sikkerhet.

I NOU 2016:19 "Samhandling for sikkerhet" kommer utvalget med en rekke forslag til hvordan dagens sikkerhetslov kan oppdateres. Det er 15 år siden sikkerhetsloven ble oppdatert sist, og det er behov for en revisjon. Verden, Norge og våre sårbarheter har endret seg kraftig i disse årene, og regelverk som skal beskytte vår nasjon må blant annet ta hensyn til et langt mer komplekst trusselbilde, en endret sikkerhetspolitisk situasjon og en svært hurtig utvikling av ny teknologi.

Det er prisverdig at utvalget i sine vurderinger forsøker å veie opp vår økende avhengighet av sikre IKT-systemer, mot hensyn til rettssikkerhet, personvern og samfunns- og bedriftsøkonomiske hensyn. Dette er ingen enkel øvelse, men slike avveininger er nødvendige, dersom vi også i fremtiden skal forbli et av verdens mest digitaliserte samfunn.

Den norske utviklingen er muliggjort av et godt samarbeid mellom myndigheter og privat næringsliv over mange år. Samarbeidet har gitt Norge et unikt fotfeste internasjonalt innenfor blant annet tyngre forsknings- og teknologimiljø. Et konkret eksempel er at verdens første LTE 4G nett var norsk. Norge har kort sagt vært i forkant i utviklingen av informasjonsteknologi, og der ønsker vi fortsatt å være. Pendelen dreier imidlertid mer i retning av at land som USA, Japan, Sør Korea og Kina inntar lederroller. Det er derfor viktig at myndighetene legger forholdene til rette for at også internasjonale aktører ønsker å drive virksomhet i Norge. Selskapene kan ikke kutte Norge som markedsområde fordi kostnadene med å tilby sine tjenester, totalt sett blir for dyre. I det store teknologiløftet med 5G, tingenes internett, Sky-tjenester, tyngre infrastrukturelle endringer og et trådløst samfunn, blir det viktig å ha et bærekraftig marked der kommersiell konkurranse fra de beste globale aktørene, har en naturlig plass. Et overordnet mål med all regulering må være at Norge beholder kompetansemiljøer, verdiskaping og sysselsetting i landet.

Abelia deler utvalgets syn på at sårbarheter som oppstår i forbindelse med digitale tjenester, skiller seg vesentlig fra tidligere tiders sikkerhetsutfordringer. Dette blant annet fordi verdikjedene til slike tjenester er lange, komplekse og kan være uoversiktlige. Hvor, hvorfor og hvordan feil oppstår kan være uklart, og feil kan forplante seg svært hurtig. Dette kan få fatale konsekvenser.

Abelia ønsker i denne høringen å komme med noen generelle betraktninger som berører flere av forslagene som framsettes. I tillegg ønsker vi å påpeke noen uklarheter på flere punkter, som vi mener det bør vektlegges i arbeidet med videre konkretisering av forslagene.

Abelia viser også til høringsinnspill fra Næringslivets Sikkerhetsråd (NSR) og fra NHO for ytterligere innspill. Vi støtter blandet annet deres forslag om å etablere en sentral mekanisme for å kontrollere, og i ytterste konsekvens stanse, utenlandske oppkjøp av selskaper som er av kritisk betydning for grunnleggende nasjonale funksjoner.

Abelias innspill

Deltakelse i norsk næringsliv

Abelia har både norske og utenlandske bedrifter med virksomhet i Norge som medlemmer. Alle bidrar til verdiskaping og sysselsetting, og for Abelia er det et viktig overordnet prinsipp at alle bedrifter bør kunne konkurrere i det norske markedet, og at disse gis lik innsikt i vilkårene for virksomhet og konkurranse.

Abelia anser utenlandske bedrifters tilstedeværelse og bidrag til norsk næringsliv som betydningsfulle og viktige på svært mange områder. Særlig for den fornyelsen og innovasjonstakten regjeringen ønsker. Innovasjon og teknologiutvikling skjer i møte mellom selskap, helt uavhengig av eierskapets nasjonalitet. Et hovedmål for myndighetene må være å bidra til at Norge er et attraktivt sted å investere og drive næringsvirksomhet, også sett med internasjonale øyne. Vurderinger av selskaper og hvilke krav disse skal underlegges og etterleve, må baseres på objektive og transparente kriterier. Det vil være svært uheldig dersom endringer i lovverk og bestemmelser skulle få utilsiktede, uheldige og fordyrende konsekvenser for næringslivet. Det er spesielt viktig at utenlandske selskaper har en klar forståelse av hvordan rammevilkårene i Norge fungerer, og blir gitt en klar forståelse av hvorfor deres bedrift eventuelt ikke kan delta i enkelte aktiviteter i Norge.

Det kan være utfordrende å skille mellom både norske og utenlandske bedrifter, og norske og utenlandske produkter. Hvilke kriterier som skal være avgjørende for å definere en bedrifts nasjonalitet er ikke gitt. Bedriftens hovedkontor, eierskapet eller ansattes nasjonalitet er alle faktorer som kan være utslagsgivende for et selskaps nasjonalitet. Et produkt eller en løsning kan inneholde en rekke elementer fra en lang verdikjede, der også underleverandører har ulik nasjonalitet. En mobiltelefons hardware kan produseres i et land, selges under et merkevarenavn som har hovedkontor i et annet land, mens 70% av innholdet på telefonen er produsert av leverandører fra en lang rekke andre land.

Abelia har stor forståelse for store deler av situasjonsbeskrivelsen i høringsnotatet NOU 2016:19 "Samhandling for sikkerhet". Vi vil således understreke viktigheten av myndighetenes ansvar for å ivareta en god balanse mellom nødvendige sikkerhetsvurderinger og transparente rammevilkår for næringslivet i Norge.

Kostnader for næringslivet.

For bedriftene vil de økonomiske konsekvensene av lovforslaget avhenge av hvilken forvaltningspraksis som etableres, og hvilke bedrifter som blir pålagt å følge loven. Det er viktig at myndighetene i det videre arbeidet gjør løpende vurderinger av hvilke kostnader de foreslåtte endringene og kravene i sikkerhetsloven medfører. Her må det også vurderes kostnadsfordeling med tanke på både små og store virksomheter. En nødvendig faktor i så øyemed er tilstrekkelig med offentlige bevilgninger for å fasilitere samhandling og etablere felles nasjonale samhandlingstjenester for sikkerhet. Kostnader for deltagelse i lovpålagt samhandlingstjenester (eksempelvis VDI samarbeid) kan finansieres av staten og ikke av den enkelte virksomhet. Utvalget gir utrykk for at både samfunnsøkonomiske og bedriftsøkonomiske lønnsomhet har vært et viktig vurderingstema. Det er bra, men Abelia vil påpeke at denne oppmerksomheten må videreføres også i det videre arbeidet med loven, ettersom dette arbeidet i større grad vil tydeliggjøre de reelle kostnadene og omfanget for lønnsomhet.

Utvalget påpeker selv i punkt 6.7.1 at med det nye forslaget til virkeområde for loven, vil flere virksomheter bli underlagt den nye sikkerhetsloven. Videre heter det at det for; *virksomheter som tidligere ikke har vært underlagt sikkerhetsloven*, vil en slik underleggelse kunne få vesentlige konsekvenser. Dette innebærer økte kostander som kan virke tyngende for den enkelte bedrift, men utvalget mener de "…sikkerhetsmessige gevinstene i et samfunnsperspektiv overstiger de ulempene en utvidelse av lovens virkeområde vil kunne få for enkelte virksomheter".[1] Spørsmålet blir da hvor stor andel av kostandene for det samfunnsmessige perspektivet

[1] NOU 2016:19 Samhandling for sikkerhet, side 113.

det er rimelig at hver enkelt bedrift skal bære byrden av. Dette er altså kostnader virksomheter blir pålagt, som går ut over de åpenbare kostnadene, sett fra et kommersielt ståsted og disse må finansieres av markedet. Mulige løsninger kan være kostnadsdifferensiering i henhold til størrelse og omsetning i bedriften. En form for kompensasjon kan være en annen. Slike løsninger bør utredes nærmere.

Det er også viktig å påpeke at leverandører som i dag leverer til bedrifter som er underlagt sikkerhetsloven, tilfredsstiller kravene ved å regulere disse i kontraktsform. Det bør drøftes grundig om og når en utvidelse av sikkerhetslovens virkeområde, jf. §2-1 til å omfatte virksomheter som «…råder over informasjon som er av kritisk betydning for grunnleggende nasjonale funksjoner», faktisk motvirker tilsiktede uønskede hendelser som kan skade grunnleggende nasjonale funksjoner jf. §1-1. Dette må sees opp mot at en foreslått utvidelse primært vil medføre negative konsekvenser i form av økte kostnader og konkurranseulemper for den enkelte bedrift. Praktiseringen av loven - og især hvilke sikkerhetstiltak som anses nødvendige og forholdsmessige - blir avgjørende for i hvilket omfang loven treffer bedriftene. Det er understreket i merknadene til formålsbestemmelsen at det ligger en plikt for sikkerhetsmyndigheten til å vurdere alternative og mindre inngripende tilnærminger til å oppnå samme effekt. Abelia legger til grunn at sikkerhetsmyndigheten og sektordepartementene følger forarbeidenes anvisning, når loven skal praktiseres.

Norske virksomheters evne til å bære sin andel av samfunnsmessige kostnader loven medfører, vil variere sterkt. Norge er et SMB land, hvilket betyr at mange mindre leverandører leverer til noen få store. Med en utvidelse av virkeområdet for loven vil en ansvars- og grenseoppgang av verdikjeder, og fordeling av kostander, være svært viktig. Dersom vi skulle komme i en situasjon der underleggelse av den nye sikkerhetsloven blir et økonomisk være eller ikke være for bedrifter, er det svært lite ønskelig. De konkrete økonomiske konsekvensene for virksomhetene, og for næringslivet som sådan, er i liten grad utredet av utvalget. Dette mener Abelia er en svakhet ved lovforslaget. Med dette mener vi at dersom påleggskompetansen i vesentlig grad blir brukt, er det altså i begrenset grad vurdert om fordelene ved loven, oppveier de omfattende pliktene som kan pålegges næringslivet.

I lovens paragraf 4.3 går det frem at det som grunnlag for virksomhetens forebyggende sikkerhetstiltak skal gjennomføres en risiko- og sårbarhetsanalyse. Virksomheten skal i forbindelse med denne kartlegge hvilke andre virksomheter den er avhengig av for å opprettholde sine grunnleggende nasjonale funksjoner. I en sikringskontekst er det mer hensiktsmessig å legge en trefaktor-modell til grunn (NS 5832:2014). Her utgjør risiko summen av verdi, trussel og sårbarhet. Begrepet risiko- og sårbarhetsanalyser i lovteksten bør også erstattes med sikringsrisikoanalyser, som er begrepet som brukes i en sikringskontekst.

Abelia har forståelse for utvalgets oppfatning av at en underleggelse av sikkerhetsloven for noen virksomheter også kan ha en positiv virkning. En slik underleggelse vil - gitt at loven fungerer etter intensjonene - innebære at virksomheten er i stand til å håndtere sikkerhetsgradert informasjon inklusiv trusselinformasjon, og kan motta konkrete råd og veiledning fra myndighetene. I enkelte sammenhenger kan dette sees på som et konkurransefortrinn og en verdibygging for den enkelte bedrift, som igjen kan gi tilgang til større markeder. Et slikt mulighetsrom vil avhenge av kostnader og omfang av det å bli underlagt sikkerhetsloven, som nevnt tidligere.

Kompetanse

Abelia har i flere år påpekt behovet for økt IT-kompetanse generelt i Norge, og økt IT sikkerhetskompetanse spesielt. Flere rapporter deriblant Lysneutvalgets rapport og nå også dette utvalgets rapport, belyser kompetansebehov på sikkerhetsområdet. I punkt 2.8[2] heter det at: "*Utvalgets forslag til innretning på den nye loven legger et stort ansvar på de enkelte fagdepartementene, og forutsetter at de ulike samfunnssektorene*

[2]NOU 2015:13 Digital sårbarhet – sikkert samfunn, side 22.

ivaretar dette ansvaret. Nøkkelbegreper i denne sammenheng er tilstrekkelig kompetanse, samt evne og vilje til samhandling og samarbeid."

Videre heter det i punkt 7.7.1[3], der systematikk for identifisering diskuteres, at: "*Som nevnt innledningsvis, mener utvalget at de enkelte departementene – i tråd med ansvarsprinsippet – bør ha det primære ansvaret for forebyggende sikkerhet innenfor sitt myndighetsområde. Sektorspesifikk kunnskap og kompetanse er av sentral betydning for å kunne identifisere de funksjoner og virksomheter som er av grunnleggende nasjonal betydning i den enkelte samfunnssektor. En avgjørende forutsetning for at en slik systematikk skal fungere i praksis, er at de enkelte fagdepartementene er sitt ansvar bevisst og følger opp det ansvaret de tillegges gjennom loven. For enkelte departementer innebærer dette behov for kompetanseheving på forebyggende sikkerhet."*

Abelia benytter igjen anledningen til å understreke hvor avgjørende det er at vi i Norge evner å heve IT-kompetansen generelt og sikkerhetskompetanse spesielt i samfunnet. Lite omfang av forskning på IKT, kommer dessuten som et resultat av relativt små kompetansemiljøer. Lysneutvalget påpeker i sin rapport at IKT-sikkerhet ikke er obligatorisk fag på alle IKT-studier her i landet. Det kan virke som det er litt tilfeldig hva norske IKT-studenter lærer om sikkerhet. De som skal bygge neste generasjons infrastruktur mangler, ifølge Lysneutvalget, grunnleggende kompetanse for sikring av IKT-systemer. Med et relativt lavt antall personer med IKT-sikkerhetskompetanse blir vi sårbare som nasjon. Et lavt antall spesialister resulterer i lite forskning også på dette området. Når også Traavik utvalget påpeker at økt og tilstrekkelig kompetanse er en forutsetning for at en ny sikkerhetslov vil fungere i praksis, bør dette være en ytterligere vekker.

Statens roller

Utvalget påpeker også en annen side av manglende kompetanse som resulterer i uklare skillelinjer mellom statens roller. Utvalget diskuterer i punkt 7.7.3[4] om det burde skilles mellom Sikkerhetsmyndighetens (NSM) rolle som fagmyndighet og rollen som tilsynsmyndighet for å sikre tilliten til uavhengigheten til tilsynsmyndigheten. Utvalget konkluderer imidlertid med videreføring av den integrerte modellen fordi "…. *at forebyggende sikkerhet mot tilsiktede uønskede hendelser er et relativt snevert fagfelt, hvor tilgangen til kvalifisert kompetanse er begrenset*".

Abelia finner det foruroligende at mangel på kompetanse brukes som begrunnelse. Tilsynsmyndighetens uavhengighet bør av hensyn til den det føres tilsyn med, ikke strande på myndighetens evne til å ansette fagfolk.

Sikkerhetsmyndigheten skal i tillegg til å være fagmyndighet og tilsynsmyndighet, også være rådgivende myndighet. En av hovedoppgavene skal ifølge utvalget være å gi informasjon, råd og veiledning til virksomheter som er underlagt loven. Abelia synes utvalget burde ha reflektert over i hvilken grad det per i dag allerede eksisterer næringsvirksomheter som driver denne typen rådgivning. Videre bør det vurderes om næringslivet - lovens sensitive sider tatt i betraktning – *kan/bør* drive slik rådgivning. I lovforslaget bør næringslivet i langt større grad sees på som en del av løsningen på utfordringene. Tiltak som bidrar til en ytterligere vekst i offentlig sektor bør være en siste utvei.

Tvisteorgan

Abelia ser i likhet med utvalget behov for at det opprettes et tvisteorgan slik at det finnes tilstrekkelige rettssikkerhetsgarantier for virksomheter som underlegges loven som rett til å bli hørt og påklage. I punkt 7.7.7 drøftes organets plassering og sammensetning nærmere. Vi savner tre ting i denne drøftelsen. For det første om også underleverandører til *grunnleggende nasjonale funksjoner* vil ha adgang til å klage til tvisteorganet. Igjen

[3] NOU 2015:13 Digital sårbarhet – sikkert samfunn, side 137.
[4] NOU 2016:19 Samhandling for sikkerhet, side 139.

mangler vurderinger rundt konsekvenser for næringslivet. For det andre om det samme tvisteorganet skal behandle både militære og sivile saker. Vi mener det bør gjøres en særskilt drøfting av om det er heldig at samme organ vurderer både militære og sivile saker. Et skille mellom militære og sivile saker gjøres på flere andre områder, blant annet når det gjelder sikkerhetsklarering av personell hvilket lovens paragraf 8-4 og 8-5 reflekterer. Og for det tredje, dersom tvisteorganet skal oppfattes som objektivt, og ha en reel rettssikkerhetsgaranti, mener Abelia i likhet med NHO og NSR at minst ett av medlemmene må komme fra det private næringsliv.

Skytjenester

I kapittel 4 diskuteres digitale sårbarheter og samfunnets avhengighet av digitale systemer og tjenester. I 4.4.3.1 side 71, heter det blant annet om offentlig sektor at "*Saksbehandling foregår etter hvert nesten utelukkende på PC eller andre digitale plattformer. Bruk av skytjenester øker i både offentlig og privat sektor så vel som hos privatpersoner. Ca. 30 % av norske næringslivaktører benytter seg av skytjenester. At denne informasjonen lagres utenfor virksomhetens lokaler fører til sikkerhetsutfordringer*"

Abelia synes dette er en svært ensidig negativ framstilling av skytjenester og sikkerhet. Det er på ingen måte gitt at bruken av skytjenester kun er en sikkerhetsutfordring. Tvert imot er det grunn til å påpeke at skylagring for en lang rekke både offentlige og private virksomheter bidrar til å *styrke* sikkerheten. Enkelt sagt er det all grunn til å tro at selskaper som spesialiserer seg på skylagring tilbyr bedre sikkerhet enn om det står en server plassert i kjelleren i virksomhetens lokaler. Det er viktig at myndighetene også ser på hvilke muligheter skylagring utgjør. Det er slik sett svært positivt at regjeringen gjennom Digital Agenda har etablert en strategi for skylagring i offentlig sektor.

***

Abelia vil avslutte med å takke for muligheten til å komme med innspill. Ta gjerne kontakt ved behov for avklaringer eller videre innspill. Vi ønsker departementet lykke til med arbeidet, og ser frem til videre dialog om disse temaene.

På vegne av Abelia,

Hilde Widerøe Wibe
Næringspolitisk direktør

Christine Korme
Direktør for digitalisering og fornying