Justis- og beredskapsdepartementet
Postboks 8005 Dep.
0030 Oslo
Ref.: 15/8216

Oslo, 14.03.2016

Høringsinnspill fra Abelia til "Digital sårbarhet – sikkert samfunn" (NOU 2015:13)

Abelia viser til høringsbrev fra Justis- og beredskapsdepartementet og leverer her våre innspill til "Digital sårbarhet – sikkert samfunn".

Om Abelia

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, vi har ca. 1750 medlemsbedrifter med 44.000 ansatte over hele landet. Abelia har medlemmer innenfor blant annet IKT, undervisning, forskning, konsulenttjenester, kreative virksomheter og interesseorganisasjoner. Flere av våre medlemmer er sentrale for digital offentlig tjenesteyting og digitaliseringsarbeid i både offentlig og privat sektor for øvrig.

Utvalgets rapport

Abelia ønsker å benytte anledningen til å rose utvalget for en meget interessant, omfattende og godt skrevet rapport. Utvalget har lykkes med å beskrive komplekse, tekniske problemstillinger på en slik måte at ikke-teknologer lett kan sette seg inn og forstå hvilke konsekvenser digitale hendelser kan ha for vår samfunnsstruktur. Norge er et av verdens mest digitalisert land. Det har gitt oss effektivitets- og samhandlingsgevinster, slik utvalget påpeker, men vi er også blitt mer sårbare. Måten vi som samfunn håndterer digitale hendelser på, er avgjørende for hvordan vi opprettholder våre verdier både som rettsstat og demokrati. Det er derfor Abelias håp at utvalgets rapport blir lest av beslutningstakere i en rekke bransjer både i privat og offentlig sektor. Helt uavhengig av hva man måtte mene om utvalgets forslag til tiltak, er denne rapporten et stykke solid folkeopplysning om et område der det er stort behov for økt bevissthet. Norge trenger et krafttak for økt datasikkerhet. Denne rapporten danner et meget godt grunnlag for videre arbeid.

To hovedområder

Abelia ønsker å påpeke to områder som er gjennomgående i så og si alle kapitler i rapporten; mangel på IKT sikkerhetskompetanse og fraværet av å se på næringslivet som en del av løsningen på de

utfordringene utvalget påpeker. Disse to områdene blir nå utdypet nærmere før andre enkelttiltak blir kommentert ytterligere.

Kompetanse

I rapportens sammendrag framheves de 9 viktigste anbefalingene utvalget kommer med. Det er påtakelig at i det i så godt som *alle* disse tiltakene er direkte eller indirekte uttalt behov for økt sikkerhetskompetanse. Det innebærer altså at en rekke av utvalgets tiltak ikke lar seg gjennomføre før Norge får økt tilgang på denne typen kompetanse. Abelia mener derfor at regjeringen i sitt videre arbeid må prioritere tiltak som gir økt kompetanse og forskning på området.

En analyse Damvad gjorde for Kommunal- og moderniseringsdepartementet i 2015 viser at Norge styrer mot generell mangel på IKT-kompetanse. Undersøkelsens "best case"-scenario gir en kraftig underdekning: 1 av 4 IKT-stillinger vil stå ubesatt i 2030[1].

Situasjonen for IKT-sikkerhetskompetanse er antatt langt dårligere. Utvalget påpeker at sikkerhet ikke er obligatorisk fag på alle IKT-studier her i landet. I grunnskolen er digitale ferdigheter like ofte forbundet med å lære seg å forbruke teknologi som å lære seg å skape med den. Det er med andre ord nærmest tilfeldig hva norske IKT-studenter lærer om sikkerhet. De som skal bygge neste generasjons infrastruktur mangler, ifølge utvalget, grunnleggende kompetanse for sikring av IKT-systemer. Denne mangelen fører også til lite forskning på området. Med et relativt lavt antall personer med IKT-sikkerhetskompetanse som fagområde og lite forskning, blir vi ikke kun sårbare som nasjon, men tilliten til vårt demokrati kan svekkes. Det illustreres godt i kapittelet som omhandler avdekking og håndtering av digitale angrep. I politiet er det i dag kun Oslo politidistrikt, KRIPOS og Økokrim som har nevneverdig kompetanse til å etterforske digital kriminalitet. Resultatet er at svært få virksomheter anmelder slike hendelser, og det svekker nødvendig tillit mellom myndigheter og borgere.

Utvalget påpeker at mangel på sikkerhetskompetanse har vært tatt opp av en rekke utvalg tidligere, inkludert Sårbarhetsutvalget i 2000. Det har likevel skjedd svært lite. Abelia mener at dersom vi virkelig ønsker å redusere den digitale sårbarheten i Norge er det svært viktig å begynne med et omfattende kompetanseløft. Vi trenger kompetansen i absolutt hele læringsløpet. Skal vi få til det må også IKT-fag, inklusive IKT-sikkerhet, inn som en del av fagene i lærerutdanningen. På bakgrunn av dette stiller Abelia seg bak samtlige forslag i rapportens kapittel om kompetanse. Blant tiltakene anser vi etablering av en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet som det aller viktigste. Vi vil også framheve forslag om å gjøre IKT-sikkerhet til obligatorisk fag på bachelorstudier for IKT, øke kapasiteten på masterutdanning innen IKT-sikkerhet og etablere en langsiktig plan for å bygge opp og vedlikeholde forskningskapasitet på området. Abelia har tidligere spilt inn behovet for en styrking av IKT-utdanningen i Norge i hele læringsløpet generelt, og rundt sikkerhet spesielt, og anser utvalgets tiltak å være i tråd med Abelias forslag til tiltak på området.

Næringslivet er en del av løsningen

I utvalgets grundige utredning er det foreslått en rekke endringer og forbedringer som innebærer at sektorielle tilsyn må øke sin kapasitet og kompetanse. Det er gjort få økonomiske beregninger av

[1] DAMVAD og Samfunnsøkonomisk analyse (2014): *Dimensjonering av avansert IKT-kompetanse*

dette. Utvalget overlater til det enkelt departement sammen med tilsynene å vurdere om det er snakk om en omdisponering av ressurser eller om det bør tilføres ekstra ressurser.

Abelia frykter at det her legges opp til en ytterligere vekst i offentlig sektor. Å sikre et godt og forutsigbart samspill mellom offentlig sektor og kunnskaps- og teknologinæringslivet handler om mer enn kapasitet. Teknologien endrer seg raskt. Det er kun gjennom å være del av den internasjonale utviklingen på IT-sikkerhetsområdet at det offentlige kan sikre seg oppdaterte løsninger og unngå innlåsing i gammel teknologi. Det skjer best gjennom å utvikle god innkjøpskompetanse og stille funksjonelle og sikkerhetsmessige krav. Abelia vil advare mot at offentlige aktører generelt og innenfor IT-sikkerhetsområdet spesielt satser på egen teknologiutvikling.

Det har uheldige virkninger når det offentlige opptrer som tilbyder i etablerte markeder for kunnskap- og teknologi. Vi ser en rekke eksempler på at nye tjenestetilbud utvikles i direkte konkurranse med næringsaktører, også innenfor IT-sikkerhetsområdet. Det offentlige er på sikt avhengig av et velfungerende norsk marked for sikkerhetsteknologi og –kompetanse. Når offentlige aktører utvikler egne produkter og tjenester som tilbys i markedet på andre betingelser enn de kommersielle aktører kan gi, undergraves på sikt næringslivets mulighet for å være en god medspiller og det offentliges tilgang på oppdatert kompetanse.

Det er en svakhet i rapporten at det er gjennomgående lite drøfting rundt hvordan næringslivet generelt og IKT-bransjen konkret kan være en del av løsningene på de utfordringene som blir påpekt. Abelia oppfordrer Justisdepartementet til å ha en nær dialog med næringslivet om hvordan de kan bidra. I den forbindelse ønsker vi å støtte særmerknad fra utvalgsmedlem Kristine Beitland i kapittel 23 der det er snakk om skytjenester. Beitland påpeker at de aktuelle departementer må ha en nær dialog med næringslivet før det utarbeides en politikk for bruk av skytjenester. Dette fordi det er viktig at myndighetene ser hvilke *muligheter* denne teknologien gir for nettopp å øke sikkerheten, og ikke ensidig fokuserer på juridiske hindringer for bruk.

Abelia mener at samarbeid mellom myndigheter og næringslivet i så stor grad som mulig bør være basert på gjensidig tillit og frivillighet. Vi er derfor usikre på om et *krav* i virksomheters årsmeldinger der ivaretakelse av IKT-sikkerhet skal beskrives er veien å gå (kapittel 19) da det kan føre til unødvendig byråkrati og kostnader for private virksomheter og ikke forenkling som ellers er regjeringens ambisjon. Frivillighet bør være utgangspunktet for deltakelse i VDI-sensornettverket som monitoreres av NSM NorCERT (kapittel 21). Det er i diskusjonen rundt frivillighet verdt å merke seg at utvalget framhever finansnæringen som "….*en sektor med høy bevissthet rundt de truslene og sårbarhetene økt digitalisering medfører*, *sammenliknet med andre sektorer*" (s. 182). Finansnæringen er en gjennomregulert bransje, men på samme tid har næringen et omfattende samarbeid aktørene i mellom gjennom felles organer og bransjeorganisasjoner. Næringens egne initiativ, samordning og standardiseringer synes å være en svært sterk driver for sektorens høye bevissthet rundt sikkerhet. FinansCERT som ble opprettet i 2013 er det eneste private cert i Norge og med 5 ansatte. Abelia synes det er grunn til å se nærmere på Finansnæringen som en modell når IKT-sikkerheten skal styrkes i andre sektorer. Igjen; næringslivet kan selv utgjøre en stor del av løsningene på en hensiktsmessig måte.

Det vil etter Abelias menings også styrke kompetansekraften til norsk næringsliv at staten/ offentlig sektor tar i bruk privat næringsliv til å løse denne type oppgaver. Et slikt samspill mellom offentlig og privat sektor vil gi norske selskaper konkurransefortrinn på et forretningsområde i sterk vekst og

med gode muligheter for norsk eksport. Ved å bygge opp kompetansen internt i offentlig sektor forblir den intern, og er dermed ikke med på å skape nye verdier for Norge utover bedret sikkerhet i offentlig sektor på kort sikt. På lengre sikt er vi bekymret for at ringvirkningene er negative også for sikkerheten i sektoren, men også for norsk næringslivs mulighet til å utvikle løsninger som kan eksporteres.

Vi registrerer med interesse at utvalget i kapittel 23 sier de har spurt flere sentrale aktører om sikkerhetskrav er til hinder for produktivitetsvekst og innovasjon, uten å få særlig klare svar. Abelia mener det vil være svært uheldig dersom næringslivet blir påført for mange omfattende og obligatoriske sikkerhetskrav fra myndighetene. Dette vil spesielt hemme innovasjon og nye bedrifter som ikke kan bære slik kostnader. Myndighetene har et ansvar for at det til enhver tid er en fornuftig balanse mellom regulering og næringsutvikling. I enhver vurdering av sikkerhetskrav må ulike hensyn avveies. Formålstjenlighet på kort og lengre sikt må stå sentralt i denne vurderingen. Å regulere seg til økt sikkerhet med utgangspunkt i dagens teknologiforståelse, kan vise seg å gi falsk trygghet, særlig på lengre sikt. Abelia er glad for at utvalget ser at en sterk IKT- sikkerhetsindustri vil være et bidrag til å redusere digital sårbarhet i Norge og at det anbefaler regjeringen å forsterke arbeidet med virkemidler for å fremme næringen. Abelia ønsker å legge til at en slik industri i Norge er en potensiell eksportvare for Norge hvor vi kan kapitalisere på vår høye tillit.

Utvalget påpeker flere steder at ansvarsfordelingen mellom etater og departementer i offentlig sektor er omfattende og kompleks. For privat sektor blir det derfor svært uoversiktlig hvem som har hvilke roller og ansvar, hva slags informasjon som kan deles, og hvilke verktøy som skal tas i bruk for utveksling av informasjon. Kort sagt: når en hendelse inntreffer er det for aktørene svært uklart hvem de skal ta kontakt med hos myndighetene, og hvem som kan bistå (Kap 21). Dette er en svært lite tilfredsstillende situasjon for aktører under angrep eller som opplever at de er i en krise. Abelia støtter derfor utvalgets mindretall som foreslår en betydelig styrking av samfunnets samlede evne til å håndtere hendelser og et langt tettere samarbeid mellom privat og offentlig sektor enn det NorCERT håndterer i dag (Kapittel 21). Mindretallet forslår på sikt å etablere et nasjonalt cybersikkerhetssenter som skal være et felles kontaktpunkt til hjelp ved hendelser.

Det er Abelias oppfatning at selv virksomheter med sentrale samfunnsroller innen energi, bank og elektronisk kommunikasjon ofte ikke får nødvendig hjelp fra norske myndigheter. Bedriftene risikerer å bli stående igjen alene i håndteringen av digitale angrep. Næringslivet må kunne kreve at myndighetene raskt informerer om kjente angrep mot bedriftenes verdier. På samme måte må myndighetene kunne kreve at næringslivet informerer om digitale angrep som kan gi bedre oversikt og mer effektiv etterforskning. Håndteringen av angrep i det digitale rom bør følge samme rutiner for roller og ansvar som ved angrep på fysiske verdier. Det betyr tettere samarbeid og bedre informasjonskanaler enn i dag. Det organiserte næringslivet har også en rolle i dette, bl.a. i å legge til rette for større grad av åpenhet og informasjonsdeling mellom næringsaktører.

Kjerneinfrastruktur

Abelia registrerer utvalgets synspunkt om at minst ytterligere en tilleggsaktør bør ha et landsdekkende kjernenett som er på samme nivå som Telenors for å redusere kritikaliteten i dennes kjerneinfrastrukturen. Utvalget begrunner dette fra et sikkerhetsperspektiv der "….*den totale summen av samfunnsverdier dette nettet bærer er uakseptabel høy".* (S 16) Et slik nett er kostnadsberegnet til 575 millioner over ti år. Anbefalingen reiser en rekke spørsmål. Før det tas noen avgjørelse i denne sammenheng oppfordrer Abelia berørte departementer til å gå i tett dialog med

aktørene selv. En rekke forhold må drøftes inngående herunder eierskap, finansiering, ansvar og forpliktelser.

Felleskomponenter

Abelia registrerer med bekymring følgende uttalelse fra utvalget i kapitelet om felleskomponenter: " *Etatene er generelt vant med å vurdere egne sårbarheter, men har i varierende grad oversikt over omfanget av eksterne aktører som er avhengige av etatens tjenester*" (s.284) Robuste og effektive felleskomponenter er en forutsetning for økt digitalisering både i offentlig og privat sektor. Abelia støtter utvalgets synspunkt om at " ….*det er problematisk at etatene alene bestemmer sikkerhetsnivået til fellesfunksjonene, uten at det sikres at de totale verdiene blir tatt hensyn til*": (s 285). Utvalget forslår å etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder og at ansvaret for dette legges under Justis- og beredskapsdepartementet. I tillegg foreslås ROS-analyser og flere underliggende tiltak. Igjen advarer Abelia mot at det her innføres et unødvendig tungt og fordyrende byråkrati og unødvendige rapporteringsrutiner. En nær dialog med eksterne virksomheter som er brukere om konsekvenser av sårbarheter, vil være en god begynnelse og en klar forbedring. I en slik dialog er det også naturlig å diskutere om næringslivet allerede besitter analyseverktøy eller andre løsninger som kan bidra til å redusere sårbarheten i felleskomponentene og konsekvensene av eventuelle hendelser.

Standarder

Abelia støtter utvalgets synspunkt om at Norge bør implementere standarder som er internasjonalt anerkjent, og at særnorske standarder er svært lite hensiktsmessig. Dette forutsetter imidlertid tett samarbeid med standardiseringsorganer i Norge, i tillegg en klargjøring av hvem som skal ha hovedansvaret for standardiseringsarbeidet i Norge. Direktoratet for forvaltning og IKT (Difi), som har ansvar for å forvalte regelverket om offentlige anskaffelser, har med utgangspunkt i egen innsikt om behov i standarder valgt å opptre som en standardiseringsinstans. Abelia mener det i stedet bør være det etablerte og uavhengige organet Standard Norge som forvalter norsk standardiseringsportefølje. Standard Norge fastsetter og utgir i dag Norsk Standard og utenlandske standarder, og organisasjonen har god erfaring i å samarbeide med en stor bredde av aktører med sterke både konkurranse- og brukshensyn. Det offentlige viser ikke tilstrekkelig lojalitet til dette, og det finnes derfor en rekke miljøer innenfor forvaltningen som utarbeider egne standarder.
Abelia har ved flere anledninger påpekt at omforente standarder må være hovedregelen og at Standard Norge er den naturlige aktøren for å utvikle nye standarder. Abelia støtter utvalgets anbefaling om at Justis- og beredskapsdepartementet har en strategisk tilnærming til hvordan det skal bidra til standardiseringsarbeidet.

Med vennlig hilsen,
Christine Korme
Direktør for Digitalisering og fornying
Abelia