Oslo, 16. januar, 2018

Høringsinnspill til IKT-sikkerhetsutvalget fra Abelia

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, vi har ca. 2200 medlemsbedrifter med omtrent 49.000 ansatte over hele landet. Abelia har medlemmer innenfor blant annet IKT, undervisning, forskning, konsulenttjenester, kreative virksomheter og interesseorganisasjoner.

Innledning

Abelia viser til IKT-sikkerhetsutvalgets brev av 9. januar der utvalget ønsker innspill til sitt videre arbeid fra virksomheter og organisasjoner. Abelia driver sammen med vårt medlem Watchcom "Forum for Digital Sikkerhet". IT-sikkerhetssjefene i omlag 40 virksomheter er i dette forumet. Fredag 2. februar inviterte forumet IKT-sikkerhetsutvalgets leder Hans Christian Holte til å holde innlegg på et frokostmøte med påfølgende diskusjon. Vi oppfordret også våre medlemmer til å komme med skriftlig innspill og sendte ut spørreskjemaet fra utvalget til alle i forumet.

Mange av spørsmålene på spørreskjemaet er trolig formulert med den enkelte virksomhet i tankene. Det er svært forståelig, men for Abelia som en medlemsorganisasjon er en del av spørsmålene vanskelig å svare direkte på. Vi velger derfor å komme med noen overordnede betraktninger vi oppfatter berører spørsmålene utvalget stiller.

Regulering

Utvalgets mandat er å vurdere om dagens regulering er hensiktsmessig for å oppnå forsvarlig IKT-sikkerhet i samfunnet. Myndighetene har i de siste årene prisverdig nok hatt en rekke utvalg og utredninger som har sett på områder som berører IKT-sikkerhet og regulering, bl a Sårbarhetsutvalget, Stortingsmelding 10 2016-2017 Risiko i et trygt samfunn og Traavikutvalget som er bakgrunnen for at vi får en ny Sikkerhetslov. Abelia er imidlertid bekymret for om det helhetlige perspektivet og totaliteten av konsekvensene av alle initiativer/regulering blir ivaretatt.

For bedriftene vil det påløpe økonomiske konsekvenser av flere regulatoriske endringer i nær framtid. Det gjelder eksempelvis GDPR og den nye Sikkerhetsloven. Foreløpig knytter det seg stor usikkerhet til sistnevnte da kostnadene av denne loven vil avhenge av hvilken forvaltningspraksis som etableres, og hvilke virksomheter som blir pålagt å følge loven. Ansvaret for IKT-sikkerhet er delt på en rekke departementer og etater. Abelia er bekymret for at disse vurderer kostnader og ulemper for egen sektor og at ingen har ansvaret for den totale belastningen for den enkelte virksomhet. Det er viktig at det gjøres løpende totale vurderinger av hvilke kostnader foreslåtte endringer og krav medfører. Det bør i denne sammenheng også gjøres en kostnadsfordeling med tanke på små og store virksomheter. Eksempelvis kan kostnader for deltagelse i lovpålagte samhandlingstjenester (eksempelvis VDI samarbeid) finansieres av staten og ikke av den enkelte virksomhet.

Flere av utredningene/utvalgene om IKT-sikkerhet har reflektert rundt kostnadsbildet. Et argument som går igjen er at de sikkerhetsmessige gevinstene for oss alle er viktigere enn kostnadene. Et

eksempel på slik argumentasjon finner vi i Traavik utvalgets NOU 2016: 19 «Samhandling for sikkerhet» der utvalget påpeker at endringer i Sikkerhetsloven kan påføre virksomheter kostnader 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 kostnadene for det samfunnsmessige perspektivet 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. Dersom IKT-sikkerhetsutvalget vurderer nye regulering må den totale påleggingen av byrder stå sentralt i betraktningen.

Det er viktig å påpeke at nødvendige sikkerhetsforanstaltninger, ikke kun ivaretas gjennom forskrifter og reguleringer. Disse kan også reguleres i kontraktsform mellom parter. Innføring av reguleringer og nye lover må sees opp mot at slike kan medføre negative konsekvenser i form av økte kostnader og konkurranseulemper for den enkelte bedrift. Alternative og mindre inngripende tilnærminger kan bidra til at vi oppnår samme effekt; økt sikkerhet og trygghet i samfunnet.

Norske virksomheters evne til å bære sin andel av de samfunnsmessige kostnadene for IKT-sikkerhets regulering vil variere sterkt. Konkrete økonomiske konsekvenser for virksomhetene, og for næringslivet som sådan, er i liten grad utredet i de utvalgene og stortingsmeldingene som er nevnt innledningsvis. Enkelt sagt; Abelia mener det må gjøres grundige vurderinger av i hvilken grad ytterligere omfattende forpliktelser for næringslivet faktisk sett bidrar til det som er en overordnet målsetting for oss alle: bedre ikt-sikkerhet. Og i hvilken grad det er rimelig at næringslivet bærer en stor del av kostnadene for vår kollektive sikkerhet.

Organisering

Reaksjonstid er avgjørende når hendelser skal håndteres. Klar operativ ledelse fra *en* myndighetsaktør ved angrep på nasjonal kritisk infrastruktur vil bidra positivt på tidsaksen og dermed redusere skadeomfanget. Abelia mener det er grunn til å legge stor vekt på hva de bedriftene som sitter i førstelinjen og ser mange av angrepene, uttaler med hensyn til organisering og klarhet i ansvarsfordeling. Telenor og Microsoft er blant de bedriftene som ved flere anledninger har uttalt at *en* myndighetsaktør bør ha totalansvaret for IKT-sikkerhet. Denne aktøren må ha kompetanse og mandat til å identifisere, analysere, håndtere og lede operativt under hendelser. Både i en normalsituasjon og ved kriser er det avgjørende at ressurser finner hverandre på tvers av sektorer. Flere bedrifter deriblant Telenor har gitt utrykk for at ressursene er for fragmentert og at miljøene primært har ansvar for informasjonsdeling og koordinering, og dermed ikke har evne og/eller mandat til hendelseshåndtering. Private aktører er selv ansvarlig for egen normalisering og håndtering av angrep også når disse er rettet mot nasjonal infrastruktur. Slik håndtering krever derfor et tett privat-offentlig samarbeid. Det bør formaliseres og gå på tvers av sektorer. Kriminelle følger ikke sektorprinsippet, da bør heller ikke vår respons kun være basert på disse prinsippene.

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

Arbeidet med å etablere et nasjonalt cyberkrim senter NC3 er nå kommet i gang. Det er bra. Abelia håper at dette er et senter som vil arbeide ut fra et helhetlig perspektiv i tett samarbeid mellom forsvar, etterretning, PST og politiet slik at ansvarlige myndigheter besitter et felles situasjonsbilde. Det vil også være ønskelig at et slik senter får en enhet der bedrifter kan henvende seg ved eventuelle cyberangrep. Det er Abelias inntrykk at det er uklart for mange av våre medlemsbedrifter hvor de skal henvende seg, hvem som har det overordnede ansvaret og hvor de kan få hjelp ved eventuelle hendelser. For privat sektor fortoner det seg 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. Dette er en lite tilfredsstillende situasjon for dem som opplever at de er i en krise. Politiet bør bli gitt ressursene og mandatet til å arbeid mot kriminalitet i cyberspace på samme måte som de gjør i den fysiske verden.

Utvalgte områder

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 politiske myndigheter har gitt utrykk for at er ønskelig. 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 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.

Kompetansemangel er en sikkerhetstrussel

Lysneutvalget påpekte i sin rapport at mangel på sikkerhetskompetanse har vært tatt opp av en rekke utvalg tidligere, inkludert Sårbarhetsutvalget i 2000. Abelia har tidligere omtalt kompetansemangelen innen IKT generelt og IKT-sikkerhet spesielt, som en varslet krise[2]. Dersom vi ønsker å redusere den digitale sårbarheten i Norge er det svært viktig å begynne med et omfattende kompetanseløft. Vi trenger IKT-sikkerhetskompetanse i absolutt hele læringsløpet. Den manglende IKT-kompetansen generelt og IT-sikkerhetskompetansen spesielt, svekker justissektoren, den svekker den almene tilliten til vår rettsoppfatning og den gjør oss som nasjon mer sårbare.

Abelia ser at fokuset på ikt-sikkerhet fra både regjering og storting har tiltatt de par siste årene. Det er blant annet kommet flere studieplasser for IKT-sikkerhet på CCIS på Gjøvik, flere IKT-studieplasser generelt og flere rekrutteringsstillinger. Dette er svært positivt, men er etter Abelias mening ikke nok. I stortingsmeldingen IKT-sikkerhet omtales en undersøkelse fra NIFU skrevet på oppdrag for Justis- og beredskapsdepartementet. Her framskrives tilbuds- og etterspørselssiden til år 2030 med en mangel på vel 4.000 personer med IKT-sikkerhetskompetanse. Abelia mener det bør opprettes 1000 studieplasser for IKT i året over en fire års periode og at en del av disse plassene bør øremerkes IKT-sikkerhet for å i større grad etterkomme etterspørselen etter kompetanse i markedet.

Kompetanseheving av allerede ansatte

Det siste året har det vært flere saker hvor uvedkommende har hatt tilgang til sensitive data om nordmenn og norske selskaper gjennom IKT-kontrakter hos blant annet Helse Sør-Øst og Direktoratet for nødkommunikasjon. Det er alvorlig hvis det på bakgrunn av disse sakene utvikler seg en ubegrunnet frykt for å kjøpe tjenester fra det private markedet eller tjenesteutsetting i offentlig sektor generelt. Mangel på kunnskap om IKT-sikkerhet kan medføre at beslutningstakere vegrer seg for å ta i bruk nettsky, frykter samarbeid med internasjonale selskaper, eller utsetter innovative løsninger fordi "noe uforutsett kan skje". En slik frykt vil hemme og forsinke den digitaliserings- og effektiviseringstakten det er behov for i offentlig sektor. Løsningen på utfordringen med utkontraktering av IKT-prosjekter er ikke å stille krav til at selskaper og ansatte skal være norske, holde utenlandske aktører ute og drive all utvikling i offentlig regi. Svaret må være å sørge for at prosjektene blir sikrere. Det skjer blant annet når det offentlige opptrer som gode bestillere og gjør nødvendige risikoanalyser hvilket krever kompetanse utover dagens nivå. Abelia merker seg at hovedtrekkene i eHelsedirektoratets rapport om tjenesteutsetting er i tråd med disse synspunktene.[3]

Utfordringene rundt tjenesteutsetting viser at det eksisterer et behov for å heve IKT-sikkerhetskompetansen hos allerede ansatte. Arbeidsgivere i både privat og offentlig sektor må prioritere etter- og videreutdanning av medarbeidere for å heve IKT-sikkerhetskompetanse. I privat sektor mener vi at en ordning med KompetanseFunn etter modell av SkatteFunn vil være en god insentivordning for å motivere bedrifter til å satse på nødvending kompetanseheving blant annet innen IKT-sikkerhet.

---

[2] https://www.abelia.no/bransjer/ikt/sikkerhet/nyheter/en-tikkende-ikt-bombe/

[3] https://www.nrk.no/norge/e-helse_-__det-er-fritt-frem-for-utflagging-av-it-i-helse-norge-1.13802322

Generell kompetanse

Mange hendelser og angrep kunne vært forhindret ved at hver enkelt av oss oppdaterer de ulike enhetene våre og er flinkere til å lage og skjule passord. Når dette gjøres i for liten grad, kan det skyldes at vi ikke forstår at handlingene til hvert enkelt individ kan beskytte oss kollektivt. Mørketallsundersøkelsen viser at manglende sikkerhetsbevissthet og kompetanse var medvirkende årsak til at 47 prosent av virksomhetenes mest alvorlige hendelser oppsto.[4] De fleste av oss har forstått gevinsten av vaksineprogrammer, men vi er fortsatt et stykke unna samme bevissthet rundt IKT-sikkerhet. Abelia har derfor tatt til orde for en folkeopplysningskampanje som har som målsetting å bedre IKT-sikkerhetskulturen generelt i Norge.

***

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 IKT-sikkerhetsutvalget lykke til med et viktig arbeid, og ser frem til videre dialog om disse temaene.

På vegne av Abelia,

Christine Korme
Direktør for digitalisering og fornying

[4] https://www.nsr-org.no/moerketall/