Justiskomiteen

Vår dato
11.12.2017

Høringsinnspill Meld. St. 38 (2016-2017) IKT-sikkerhet – Et felles ansvar

Digitaliseringen gjør det norske samfunnet tryggere, men samtidig sårbart på nye måter. Vi må forholde oss til risiko for menneskelige og tekniske feil, så vel som bevisste handlinger utført av aktører som vil manipulere, lamme eller på annen måte ramme staten Norge, samfunnet og borgerne.

Telenor Norge AS (heretter Telenor) eier og forvalter samfunnskritisk infrastruktur, som sammen med våre tjenester innen mobil, fastnett og bredbånd er kritiske for at det norske samfunnet skal fungere. Nesten 80 prosent av all datatrafikk i Norge går gjennom vår infrastruktur. Det gir oss et betydelig samfunnsansvar og betyr at vi må levere stabile og trygge tjenester, og at vi er et mål for trusselaktører. Cybersikkerhet er derfor et strategisk kompetanse- og satsingsområde for Telenor, for å sikre en mest mulig motstandsdyktig digital infrastruktur.

Telenor er opptatt av å samarbeide godt med myndighetene om digital sikkerhet og det gjør vi på flere områder. Vi ser imidlertid at den nasjonale evnen til å håndtere hendelser i cyberspace er for fragmentert. Vi er derfor positive til meldingens intensjon om å *styrke samarbeidet mellom private og offentlige virksomheter, og mellom sivil og militær sektor.*

Kapittel 5 Et felles ansvar

Et godt nasjonalt sikkerhetsarbeid krever samarbeid mellom mange aktører som må formaliseres for å kunne gi effekt. I dag er samarbeidet fragmentert og mer dugnadsorientert enn forpliktende. Samhandling mellom norske sikkerhetsmyndigheter, Forsvaret, Politiet og andre naturlige samarbeidspartnere i sivil sektor er avgjørende for sikkerhetsnivået i Norge. I hele krisespekteret, fra normalsituasjon til en faktisk hendelse treffer samfunnskritiske funksjoner, er det avgjørende at ressursene er i stand til å finne hverandre for å redusere mulig konsekvens så effektivt som mulig. Myndighetene har etablert et rammeverk for håndtering av digitale hendelser, hvor private samfunnskritiske virksomheter er utelatt. Rammeverket er en start, men det må jobbes aktivt med og utvikles videre for at nasjonen effektivt kan håndtere digitale trusler.

Vi mener at det å forstå hendelser i cyberspace, og håndtere dem med minst mulig konsekvens for staten, samfunnet og borgerne, bør være en viktig oppgave for Totalforsvaret. Det er positivt at Telenor igjen er blitt invitert inn i Sentralt totalforsvarsforum. Aktører med samme samfunnskritikalitet må også få plass.

Meldingen varsler også regjeringens plan om å etablere et bedre offentlig-privat samarbeid gjennom Forum for IKT-sikkerhet. Vi mener det er viktig at aktører som deltar i dette fora forvalter samfunnskritisk infrastruktur eller innehar en samfunnskritisk funksjon. Dette tror vi er avgjørende for at vi skal kunne treffe tiltak på rett nivå for samfunnet og borgerne.

Kapittel 6 Forebyggende IKT-sikkerhet – virksomheters egenevne

Myndighetene har gjennom offentlige anskaffelser av digitale tjenester rom for både å stimulere til investeringer i sikkerhet og selv sørge for økt trygghet for egen virksomhet. Dersom anbudsrunder vekter pris i for stor grad, er det risiko for at det går på bekostning av sikkerhet. Det må i større grad etterspørres og vektes forhold knyttet til sikkerhet i offentlige anskaffelser. Dette vil bidra til tryggere digitale tjenester.

Telenor Norge AS
Fornebu, Bærum

Kontoradresse:
Snarøyveien 30
1360 Fornebu

Postadresse:
P.O. Box 800
1331 Fornebu

Telefon:
810 77 000
Telefaks:
23 16 60 10

Bankgiro:
7058 06 66947

Hovedkontor:
Snarøyveien 30
1360 Fornebu
Organisasjonsnummer:
NO 976 967 631 MVA

Kapittel 7 Avdekke og håndtere digitale angrep

Én offentlig myndighetsaktør bør ha totalansvar for IKT-sikkerhet. Aktøren må ha kompetanse til å identifisere, analysere og håndtere trusselaktørers forsøk på påvirkning av Norge og norske interesser, samt evne til å lede håndtering av hendelser. Sektorprinsippet må ikke være et hinder for effektiv styring og ledelse. I cyber er reaksjonstid avgjørende og vi mener at det er vesentlig at justis- og forsvarssektoren også her sitter tett sammen for å ha et felles situasjonsbilde.

De operative beredskapskapasiteter som finnes i myndighetsapparatet må understøtte håndteringen av cyberoperasjoner mot nasjonal infrastruktur – også når denne er eid av private aktører, som selv er ansvarlig for håndtering og normalisering. Dette underbygger behovet for formalisering av privat-offentlig samarbeid på tvers av sektorer. Norge har i tillegg etablert et stort antall sektorvise responsmiljøer uten egen evne til å håndtere hendelser, kun med mandat til informasjonsutveksling og koordinering. Telenor mener at den operative evnen ikke er tilpasset hva det er behov for.

Kapittel 9 Kritisk infrastruktur

Stortinget har for 2018 bevilget 40 millioner kroner til etableringen av et pilotprogram for å demonstrere sikkerhetsbehov og kommersielt grunnlag for investeringer i kjernenett med formål å øke den samlede nasjonale kapasiteten og sikkerheten i ekomnettene. Heller enn å binde seg for entydig til ett bestemt mål/en bestemt løsning, bør piloten se på ulike måter å nå det overordnete målet; å øke robusthet i nettene våre uten å gripe for my**e** inn i konkurransen i markedet.

Telenor Norge anbefaler at pilotprogrammet gjennomføres med klart formål om å styrke den nasjonale transportnettinfrastrukturen, og at et bredt utvalg tiltak vurderes for å realisere dette – også forsterkninger av eksisterende infrastruktur og kjernenett, der dette kan gi best effekt. Tilgjengelige midler må benyttes på de mest effektive tiltakene for å redusere kritisk sårbarhet og for å styrke digital robusthet og sikkerhet

Kapittel 20 Digitale angrep

Telenor mener det er positivt at arbeidet med å etablere et nasjonalt cyber crime center (NC3) kommer i gang. Det blir avgjørende at dette får mandat, verktøy og ressurser som trengs for å bekjempe kriminalitet i cyberspace. Samtidig opplever vi at grensene kan være både uklare og uoversiktlige mellom hva som er å betrakte som kriminell aktivitet under politiets ansvar, og andre ondsinnede hendelser i cyberspace, som f.eks. kan være rettet mot Norge som nasjon. Vi er derfor av den oppfatning at et slikt senter bør ha en helhetlig tilnærming, der både Sikkerhetstjeneste (PST), Forsvaret, og Etterretningstjenesten arbeider operativt sammen for å skape en felles situasjonsforståelse.

Telenor takker for muligheten til å komme med innspill, og bidrar gjerne med mer informasjon om komiteen ønsker det i sin videre behandling av saken.

Med hilsen
Telenor Norge AS

Hanne Tangen Nilsen,
Sikkerhetsdirektør

Kontaktpersoner for Telenor Norge
Benedicte Økland, Myndighetskontakt: btno@telenor.com - 454 19 389
Fredrik Wang Gierløff, Myndighetskontakt: fwg@telenor.com - 92 02 96 77