Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Mottakerliste

Vår ref.: 1301722-1 -

Vår dato: 2.4.2013

Deres ref.:

Deres dato:

Saksbehandler:
Svein Sundfør Scheie

www.npt.no

Ekomlovens krav vedrørende kommunikasjonsvern, integritet og tilgjengelighet - logiske angrep

1. Innledning

Post- og teletilsynet (PT) ser behovet for å kommunisere de risikoakseptkriterier som gjelder etter ekomloven §§ 2-7, 2-9 og 2-10 i forhold til trusselen for logiske angrep mot konfidensialiteten, integriteten og tilgjengeligheten i og til ekomnett og -tjenester. I denne sammenheng forstås angrep slik at det både omfatter tjenestenektangrep eller lignende, og hel eller delvis ekstern overtakelse av funksjon eller kapasitet hos en tilbyder.

Dette brev omhandler kun de plikter en tilbyder er underlagt i medhold av ovennevnte bestemmelser i ekomloven, og kommer i tillegg til andre spesifiseringer av ekomloven.

2. Ekomloven § 2-7 Kommunikasjonsvern med forskrifter

Etter ekomloven § 2-7 er en tilbyder pliktig å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i egne elektroniske kommunikasjonsnett og -tjenester. Trafikkdata skal slettes eller anonymiseres så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål, med mindre annet er bestemt i eller i medhold av lov. Annen behandling av trafikkdata krever samtykke fra bruker. I ekomforskriften er det gitt ytterligere regler for behandlingen av trafikkdata på tilbyderens hånd.

Hvorvidt konfidensialiteten brytes vil kunne være vanskelig å avdekke, særlig gjelder dette hvis den eller de som bryter konfidensialitetsplikten ikke på noen offentlig måte avslører at denne plikten er brutt. For å sikre seg mot dette, vil det måtte etableres sikkerhetsforanstaltninger som i tilstrekkelig grad forhindrer brudd på konfidensialiteten. Dette kan være fysiske, personellmessige og/eller logiske sikkerhetsforanstaltninger. Effekten av logiske sikkerhetsforanstaltninger vil blant annet også være avhengig av hvem som har etablert disse (både software- og hardwaremessig) og graden av kontroll tilbyder beholder over sine systemer. Hva som er tilstrekkelige sikkerhetsforanstaltninger vil være en skjønnsmessig vurdering, hvor betydningen av den tjeneste eller nett som vurderes har, tillegges stor vekt.

I Ot prp nr 58 (2002-2003) side 92 første spalte uttales om dette skjønnet:

> *«Ved vurderingen av hva som er nødvendig sikkerhetstiltak skal det ses hen til hva som er den beste løsning på markedet til enhver tid («state of the art») og kostnadene ved*

Besøksadresse | Office address
Nygård 1 Lillesand

Postadresse | Postal address
Postboks 93, 4791 Lillesand

+47 22 82 46 00
firmapost@npt.no

Fax: +47 22 82 46 40
Org.nr: NO 974 446871

iverksettelse av denne løsningen. I vurderingen av hvilken sikkerhet som skal tilbys gjelder med andre ord prinsippet om forholdsmessighet mellom kostnadene og sikkerheten som oppnås. På bakgrunn av dette skal tilbyder yte en sikkerhet som er tilpasset risikoen. Om nødvendig må tilbyder av nett og tilbyder av tjeneste samarbeide om sikkerheten.»

Det er et utall av risiki som kan medføre ikke-overholdelse av konfidensialitetsplikten. Uten å gi noen uttømmende liste over hvilke risiki en tilbyder må iverksette sikkerhetstiltak mot, holder det i dette brev å slå fast at også trusselen om angrep mot konfidensialiteten i elektronisk kommunikasjon fra meget kompetente organisasjoner, også gjennom en tilbyders (potensielle) underleverandører omfattes. Dette innebærer at en tilbyder ikke kan se bort ifra denne trusselen, og følgelig må iverksette tiltak for å redusere mulige skadevirkninger av denne. Det understrekes at det ikke forventes at en tilbyder iverksetter tiltak mot konkrete trusler om spionasje fra fremmede stater uten at relevante norske myndigheter har informert tilbyderen om dette. Det påhviler imidlertid en tilbyder en egen plikt til å etterspørre relevant myndighet om slik informasjon ved større utstyrsanskaffelser eller annen signifikant endring i infrastruktur eller driftskonsept.

Ett viktig unntak fra konfidensialitetsplikten er den plikten som følger av ekomloven § 2-8. Unntaket etter ekomloven § 2-8 kan imidlertid ikke trekkes lengre enn hva norsk lov til enhver tid tillater.

3. Ekomloven § 2-9 Taushetsplikt

Etter ekomloven § 2-9 er en tilbyder pliktig å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter. De plikter å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder får anledning til selv å skaffe seg kjennskap til slike opplysninger. Opplysningene kan heller ikke nyttes i egen virksomhet eller i tjeneste eller arbeid for andre, med unntak av statistiske opplysninger om nettrafikk som er anonymisert og ikke gir informasjon om innretninger eller tekniske løsninger. Taushetsplikt gjelder også for enhver som utfører arbeid eller tjeneste for tilbyder av elektronisk kommunikasjonsnett eller -tjeneste, installatør, teknisk kontrollorgan eller myndigheten, også etter at vedkommende har avsluttet arbeidet eller tjenesten.

I ekomforskriften er det gitt ytterligere regler for behandlingen av trafikkdata på tilbyderens hånd, herunder krav om at de som skal ha tilgang til trafikkdata skal være bestemte personer som må ha fullmakt til utførelsen av slikt arbeid fra tilbyderen. Behandlingen av trafikkdata skal begrenses til arbeidet med fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektronisk kommunikasjonstjeneste eller avsløring av urettmessig bruk av elektronisk kommunikasjon. Det er inntatt noen unntak fra taushetsplikten i ekomloven § 2-9, som imidlertid ikke anses relevante i denne sammenheng.

Hvorvidt taushetsplikten faktisk brytes, vil kunne være vanskelig å avdekke, særlig gjelder dette hvis den eller de som krenker taushetsplikten ikke på noen offentlig måte avslører at denne plikten er brutt. For å sikre seg mot dette, vil det måtte etableres sikkerhetsforanstaltninger som i tilstrekkelig grad forhindrer brudd på taushetsplikten. Dette kan være fysiske, personellmessige og/eller logiske sikkerhetsforanstaltninger. Effekten av logiske sikkerhetsforanstaltninger vil blant annet også være avhengig av hvem som har etablert disse (både software- og hardwaremessig) og graden av kontroll tilbyder beholder over sine systemer. Hva som er tilstrekkelige sikkerhetsforanstaltninger vil være en skjønnsmessig vurdering, hvor betydningen av den tjeneste eller nett som vurderes har, tillegges stor vekt.

Ekomloven § 2-9 er i stor grad en videreføring av teleloven § 9-3. I forbindelse med vedtakelsen av denne bestemmelsen ble det uttalt i Ot.prp. nr. 36 (1994-95) side 43-44, bl.a. følgende om hva taushetsplikten omfatter:

"Taushetsplikten gjelder andres bruk av telekommunikasjon generelt, som foruten konsesjonsbelagte ytelser omfatter bruk av tilslutningsnett eller andre ikke-konsesjonspliktige telenett, herunder overføringsnett for kringkasting og konkurransetjenestene. Også valg av tekniske løsninger i forbindelse med etablering av nett og utstyr skal det bevares taushet om. "Andres" (bruk) er egne ansatte og kunders og andre forretningsforbindelser, samt alle andre personers, bedrifters eller myndigheters bruk av telekommunikasjon. Taushet om "innholdet

av telekommunikasjonen" gjelder i tillegg til forbud mot å offentliggjøre informasjon som følger av straffeloven og personregisterloven. Taushetsplikten innebærer også plikt til aktivt å hindre at uvedkommende får tilgang til opplysningene. (vår understreking)»

I tillegg til at taushetsplikten forbyr tilgang til taushetspliktig informasjon fra «uvedkommende», innebærer taushetsplikten sammen med konfidensialitetsplikten også at så få som mulig gis tilgang til denne type informasjon. Dette følger av kravet om særlig autorisasjon av personell som skal ha tilgang til trafikkdata. Kravet om særlig autorisasjon av personer som skal ha tilgang til trafikkdata innebærer også at en tilbyder må ha et bevisst forhold til hvem selskapet gir tilgang til taushetspliktig informasjon. I denne sammenheng innebærer det at selskapet må dokumentere at de som får tilgang til slik informasjon har tjenestelig behov, anses personlig egnet og vil overholde taushetsplikten. Jo fjernere vedkommende som får tilgang til tauhetspliktig informasjon er fra norsk rettstradisjon og mulig håndhevelse, jo strengere må en tilbyders sikkerhetstiltak være for å tilfredsstille kravet om taushetsplikt. Begrensning i spredningen av taushetspliktig informasjon er også et sentralt tiltak for å sikre overholdelsen av plikten.

Det er et utall av risiki som kan medføre ikke-overholdelse av taushetsplikten. Uten å gi noen uttømmende liste over hvilke risiki en tilbyder må iverksette sikkerhetstiltak mot, holder det i dette brev å slå fast at også trusselen om angrep mot informasjonen i elektronisk kommunikasjon underlagt taushetsplikt fra meget kompetente organisasjoner, også gjennom en tilbyders (potensielle) underleverandører omfattes. Dette innebærer at en tilbyder ikke kan se bort ifra denne trusselen, og følgelig må iverksette tiltak for å hindre at uvedkommende får tilgang til opplysningene, og å redusere skadevirkningene dersom dette likevel skulle inntreffe. Det understrekes at det ikke forventes at en tilbyder iverksetter tiltak mot konkrete trusler om spionasje fra fremmede stater uten at relevante norske myndigheter har informert tilbyderen om dette. Det påhviler imidlertid en tilbyder en egen plikt til å etterspørre relevant myndighet om slik informasjon ved større utstyrsanskaffelser eller annen signifikant endring i infrastruktur eller driftskonsept.

Ett viktig unntak fra taushetsplikten er den plikten som følger av ekomloven § 2-8. Unntaket etter ekomloven § 2-8 kan imidlertid ikke trekkes lengre enn hva norsk lov til enhver tid tillater.

4. Ekomloven § 2-10 Sikkerhet og beredskap med forskrifter

Etter ekomloven § 2-10 skal tilbyder tilby elektronisk kommunikasjonsnett og -tjeneste med nødvendig sikkerhet for brukerne i fred, krise og krig. Tilbyder skal opprettholde nødvendig beredskap, og viktige samfunnsaktører skal prioriteres ved behov. Tilbyder skal formidle viktig melding fra statsmyndighet.

Bestemmelsens innhold er nærmere (dog ikke uttømmende) spesifisert i klassifiseringsforskriften.

Sikkerhetsnivået som følger av ekomloven § 2-10 med forskrifter er satt for å sikre tilgjengeligheten av ekomtjenester til norske brukere i fred, krise og krig. Hvor normen skal settes er utdypet i Ot prp nr 58 (2002-2003) side 94 som følger:

«Bestemmelsen setter krav til tilbyder om sikring av elektroniske nett og tjenester (offentlige og private) i situasjoner som går utover det som aktørene selv forventes å ville sikre seg mot ut fra et rent kommersielt synspunkt. Bestemmelsen er ment å supplere sikkerhetsloven (lov 20.04.98 nr. 10). For sikkerhet knyttet til konfidensialitet vises det til § 2-7 om kommunikasjonsvern. Bestemmelsen viderefører blant annet adgangen til å pålegge samfunnspålagte oppgaver i beredskapssammenheng. Øvrige samfunnspålagte oppgaver reguleres i § 5-3.

Med kravet om nødvendig sikkerhet for bruker i første ledd menes at nett og tjenester skal sikres på en slik måte at bruker, selv i situasjoner der nettet utsettes for ekstraordinære påkjenninger, så langt som mulig skal kunne benytte grunnleggende elektroniske kommunikasjonstjenester. I vurderingen av om nødvendig sikkerhet er oppnådd skal det tas hensyn til kostnadssiden ved å sikre elektroniske kommunikasjonsnett og -tjenester. Det legges opp til at viktige samfunnsaktører skal prioriteres ved behov.»

Bestemmelsens formål er altså å redusere muligheten for bortfall eller vesentlig reduksjon av tilgjengeligheten av ekomtjenester for brukere, da konfidensialiteten og taushetsplikten reguleres av ekomloven §§ 2-7 og 2-9. Bestemmelsen setter krav til at nett og tjenester skal kunne motstå ytre og indre ekstraordinær påkjenning og påvirkning. Dette vil omfatte påkjenninger fra vær, bortfall av primær strømforsyning, hærverk og brudd i sambandsføringer, samt maskinvarefeil. Bestemmelsen omfatter også sikkerhet for å unngå bortfall på grunn av logiske feil eller angrep. I denne sammenheng forstås angrep både å omfatte tjenestenektangrep eller lignende, og hel eller delvis ekstern overtakelse av funksjon eller kapasitet hos en tilbyder.

Uten å gi noen uttømmende liste over hvilke risiki en tilbyder må iverksette sikkerhetstiltak mot, holder det i dette brev å slå fast at også trusselen om logiske angrep fra meget kompetente organisasjoner, også gjennom en tilbyders (potensielle) underleverandører omfattes. Dette innebærer at en tilbyder ikke kan se bort ifra denne trusselen, og følgelig må iverksette tiltak for å redusere mulige skadevirkninger av denne. Det understrekes at det ikke forventes at en tilbyder iverksetter tiltak mot *konkrete* trusler om logiske angrep fra fremmede stater uten at relevante norske myndigheter har informert tilbyderen om dette. Det påhviler imidlertid en tilbyder en egen plikt til å etterspørre relevant myndighet om slik informasjon ved større utstyrsanskaffelser eller annen signifikant endring i infrastruktur eller driftskonsept.

5. Særlig om utkontraktering

Stadig flere av funksjonene som tradisjonelt har vært ivaretatt av tilbyderen selv, utsettes i dag til eksterne (under)leverandører. Med eksterne leverandører innebefattes også selskaper som direkte eller indirekte har samme eierselskap som tilbyder. Det understrekes at en tilbyder ikke kan, gjennom utsetting av driften av deler av sin tjenesteleveranse eller virksomhet, begrense sitt ansvar for overholdelse av pliktene etter ekomloven.

Det følger av ekomloven § 10-1 at myndigheten skal føre tilsyn med at krav fastsatt i eller i medhold av ekomloven er oppfylt. Myndigheten kan nytte bistand fra andre ved utførelsen av tilsynet og kan ta stikkprøver og foreta målinger og annen kontroll uten forhåndsvarsel. Det følger videre av ekomloven § 10-3 at myndigheten kan kreve opplysninger som er nødvendige for gjennomføringen av ekomloven, vedtak gitt i medhold av loven, eller forpliktelser som følger av internasjonale overenskomster som Norge har sluttet seg til. Tilbyder skal videre på forespørsel fra myndigheten gi opplysninger, herunder sikkerhetsgraderte opplysninger om elektroniske kommunikasjonsnett og -tjenester, og om infrastruktur knyttet til drifts- og styringssystemene. Opplysningene kan kreves utlevert skriftlig eller muntlig innen en fastsatt frist. Etter ekomloven § 10-4 har den som er gjenstand for tilsyn plikt til å sørge for at myndigheten har uhindret adgang til virksomheten og lokaler med utstyr for elektronisk kommunikasjon. Nødvendig dokumentasjon skal gjøres tilgjengelig for myndigheten. Innehaver eller dennes representant kan pålegges å være til stede under tilsynet. Tilbydere kan heller ikke iverksette utkontrakteringer som medfører at selskapet ikke kan overholde disse bestemmelsene.

Avslutningsvis understrekes for ordens skyld at forståelsen av ekomloven §§ 2-7, 2-9 og 2-10 som fremkommer her, også vil ha gyldighet hvis lovendringsforslagene fremmet i Prop 69 L (2012-2013) blir vedtatt.

Med hilsen

Torstein Olsen
direktør

Einar Lunde
avdelingsdirektør