Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Stockholm den 28 maj 2024

Telenors svar i remiss av utredning om nya regler om cybersäkerhet Fö2024/00496

Telenor Sverige AB (Telenor) lämnar följande svar i regeringens remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Inledning

Utredningen föreslår i delbetänkandet en ny lag om cybersäkerhet som ska träffa verksamheter i ett antal utpekade sektorer och bl.a. ersätta motsvarande säkerhetsbestämmelser i lagen om elektronisk kommunikation. Cybersäkerhetslagen ska i stor utsträckning kompletteras genom myndighetsföreskrifter.

Cybersäkerhetslagen bygger på NIS2-direktivet som har till syfte att främja den inre marknaden genom harmoniserade krav och processer som ska säkerställa en hög nivå av säkerhet för nätverks- och informationssystem.

Telenor bedriver idag ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete bl.a. baserat på lagen om elektronisk kommunikation och föreskrifter meddelade av Post- och telestyrelsen (PTS). Telenor är därtill certifierade enligt ISO 27001 ledningssystem för informationssäkerhet.

Telenors synpunkter på utredningens förslag

Utredningen föreslår att cybersäkerhetslagen ska träda i kraft den 1 januari 2025. Några övergångsbestämmelser föreslås inte. Vid samma tidpunkt ska 8 kap. 1 – 4 §§ lagen om elektronisk kommunikation upphävas. Cybersäkerhetslagens bestämmelser måste i hög utsträckning kompletteras med myndighetsföreskrifter. Telenor finner det osannolikt att samtliga föreskrifter kan finnas på plats den 1 januari 2025 och menar att en mer rimlig tid för lagen att träda i kraft är den 1 juli 2025, alternativt att lagen träder i kraft men att den tillämpas på relevanta verksamhetsutövare från den 1juli 2025 och att tidigare gällande bestämmelser övergångsvis gäller fram till dess. Det faktum att ett snabbt genomförande är önskvärt för att Sverige ska slippa ett överträdelseförfarande är inte argument nog för att forcera fram regelverket utan att föreskrifter och annan vägledning beretts med sedvanlig omsorg.

Telenor ser en fördel om regelverket för telekomsektorn, som idag är inarbetat och fungerar väl, inte ändras för mycket med krav och processer spridda i en mängd olika författningar och under ett flertal tillsynsmyndigheters ansvar. Kraven på säkerhetsarbete och säkerhetsåtgärder för telekomsektorn hade med fördel kunnat kvarstå i lagen om elektronisk kommunikation och PTS skulle kunna ges föreskriftsrätt och tillsynsansvar för samtliga krav som gäller för sektorn. Generella bestämmelser som träffar flera sektorer blir mindre tydliga och konkreta än sektorsspecifika regler, och myndigheter med tillsyn över en stor mängd sektorer blir mindre specialiserade och träffsäkra.

Av förslaget till 1 kap. 13 § framgår att om en enskild verksamhetsutövare i delar bedriver säkerhetskänslig verksamhet gäller i de delarna inte kraven på riskhanteringsåtgärder och incidentrapportering enligt 3 kap. Telenor kan ha förståelse för strävan att undvika dubbel reglering, men kan inte se att cybersäkerhetslagen och säkerhetsskyddslagen reglerar samma riskhantering. Det allriskperspektiv som genomsyrar cybersäkerhetslagen finns inte i säkerhetsskyddslagen och dessutom kan en verksamhets betydelse för Sveriges säkerhet ändras i takt med den underliggande säkerhetsskyddsanalysen. Därtill kan det röra sig om samma verksamhet som i vissa relationer är av betydelse för Sveriges säkerhet men i andra relationer saknar sådan betydelse. Telenor ser därför att det ligger mer i linje med NIS2-direktivets syften att all verksamhet som ligger inom de utsedda sektorerna ska följa Cybersäkerhetslagens bestämmelser om riskhanteringsåtgärder och incidentrapportering och att eventuella säkerhetskänsliga uppgifter inom ramen för en tillsyn kan behandlas av myndigheten med tillbörlig sekretess.

Av förslaget till 3 kap. 2 § framgår att verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Begreppet ”informationssäkerhet” är inte definierat men Telenor utgår från att man här menar alla aspekter av säkerhet som kan påverka tjänster och information, dvs även rena nätsäkerhetsaspekter. Då det befintliga regelverket genom PTS nätsäkerhetsföreskrifter har tydliga krav och inarbetad praxis gällande säkerhetsarbetet för nättillgångar och förbindelser, framstår det som något oklart hur omfattande kraven blir enbart med hänvisning till ”informationssäkerhet”. Avgränsningen måste göras tydlig, då PTS behöver särreglera det som eventuellt blir över, såsom krav på robusthet och redundans.

Av förslaget till 3 kap. 4 § framgår att en incident ska anses betydande om den orsakat eller kan orsaka en allvarlig driftstörning eller en ekonomisk skada för verksamhetsutövaren. Att en omständighet potentiellt skulle kunna orsaka en driftstörning eller ekonomisk skada är en bedömningsfråga om vad som kan hända men som inte hänt. För att verksamhetsutövarna ska kunna anmäla icke-materialiserade risker som kan leda till incidenter krävs tydlig och konkret vägledning.

Vidare framgår att det ska anses vara en betydande incident om den vållar eller kan vålla en betydande materiell eller immateriell skada för andra. Det kan i många fall vara svårt eller omöjligt för en verksamhetsutövare att bilda sig en uppfattning om en incident som påverkar andra kan vålla denne betydande skada. Uppdelningen i materiella och immateriella skador verkar vara hämtad från dataskyddsförordningens skadeståndsregler och kan ifrågasättas i sammanhanget. Det finns ett behov av föreskrifter som tydliggör hur verksamhetsutövaren ska bedöma sina incidenters påverkan för andra.

När det gäller incidentrapporter ska verksamhetsutövaren redan inom 24 timmar uppmärksamma CSIRT på en betydande incident, något som utredningen kallar en ”varning”. Begreppet känns missledande då det inte är fråga om en varning i ordets normala betydelse, utan snarare en indikation. Det ska här understrykas att det inom 24 timmar från en upptäckt avvikelse ofta återstår mycket analysarbete innan det går att konstatera att en betydande incident inträffat. 24-timmarsfristen är också utmanande då merparten verksamhetsutövare inte har full bemanning dygnet runt årets alla dagar. Det framstår vidare som en otydlig lydelse i 5 § andra meningen där det sägs att det ”ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter”. En bättre lydelse kan vara verksamhetsutövaren ”ska särskilt ange om det finns misstanke om att incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter”.

Då ”varningen” är sanktionsgrundande kommer det sannolikt inkomma mer av dessa indikationer än vad som sakligt är motiverat, vilket aktualiserar behov av att kunna dra tillbaka varningen om det vid närmare analys inte visar sig vara fråga om en betydande incident.

Utredningen föreslår i 4 kap. 8 § att tillsynsmyndigheten får, om det finns särskilda skäl, ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ genomföra en riktad säkerhetsrevision. Tillsynsmyndigheten får också själv anlita ett oberoende organ för regelbundna säkerhetsrevisioner. Ett sådan åtgärd är mycket ingripande och det måste finnas många och allvarliga indikationer på brister för att motivera dylika beslut. Telenor föreslår därför att det i bestämmelsen anges att det ska krävas synnerliga skäl.

På sidan 125 lyfts frågan om det är verksamhetsutövarens verksamhet i dess helhet som omfattas eller om det är relevanta delar av verksamheten som behöver uppfylla direktivets krav. Här landar utredningen i att det är all verksamhet som ska omfattas, även sådan verksamhet som inte omfattas av de utpekade sektorerna. Det leder till att kraven på riskhanteringsåtgärder och incidentanmälan smittar av sig på verksamheter som inte annars hade lytt under lagen, bara av den anledningen att det är samma entitet som utövar de olika verksamheterna. Detta kan inte ha varit lagstiftarens intention. Utredaren motiverar sitt ställningstagande bl.a. med åsikten att nätverks- och informationssystem många gånger är sammankopplade inom hela verksamheten och att incidenter inom en del kan påverka en annan del. Telenor menar att om det skulle vara så att kritisk verksamhet kan påverkas av störning i helt annan verksamhet så kan verksamhetsutövarens säkerhetsarbete ifrågasättas redan på den grunden. Telenor anser i stället att lagen endast ska vara tillämplig på verksamhet som tydligt ingår i de identifierade sektorerna. Så gäller exempelvis under lagen om elektronisk kommunikation idag. Att utöka tillämpningsområdet till väsensskilda verksamheter utanför de identifierade sektorerna är inte proportionerligt och kan dessutom skapa snedvridningar och konkurrensproblem.

Av 5 kap. 2 § framgår bl.a. att ett ingripande kan ske genom att tillsynsmyndigheten meddelar en anmärkning. Det anges på s. 250 att det ska vara obligatoriskt att meddela en anmärkning om inget annat ingripande görs. Självfallet måste detta endast gäller om tillsynen identifierar brister eller underlåtelser. En tillsyn ska ju även kunna avslutas utan något ingripande. För smärre brister och ursäktliga tillkortakommanden

som rättas omedelbart bör det också vara möjligt att avsluta tillsynen utan ingripanden. Det ska här lyftas fram att en formell anmärkning kan få negativa effekter för en verksamhetsutövare i relation till sina kunder, presumtiva kunder och i upphandlingsförfaranden.

Av sid. 178 i utredningen följer att väsentliga och viktiga verksamheter inom elektronisk kommunikation ska anmäla sig till PTS, som upprättar ett nytt register. Det är inte tillräckligt med det register som redan finns för tillhandahållare av elektroniska kommunikationsnät och -tjänster, då cybersäkerhetslagen innebär att nya uppgiftskategorier samlas in. Telenor ser gärna att PTS hanterar båda dessa register.

När det gäller frågan om vilken myndighet som ska meddela föreskrifter om riskhanteringsåtgärder och det systematiska säkerhetsarbetet menar Telenor att starka skäl talar för att PTS ska vara den myndighet som även fortsättningsvis har föreskriftsrätt för sektorn elektronisk kommunikation. Detta föreslås av utredningen och ligger också i linje med beaktandesats 95 i NIS2-direktivet.

För närvarande är det PTS som meddelar föreskrifter om incidentrapportering, med undantag för integritetsincidenter som rapporteras enligt bestämmelser i en EU-förordning. Telenor ser fördelar med att PTS även fortsättningsvis beslutar föreskrifter om incidentrapportering för sektorn elektronisk kommunikation. På samma sätt ser Telenor fördelar med att verksamhetsutövare inom sektorn elektronisk kommunikation rapporterar incidenter till PTS. Det är PTS som i egenskap av tillsynsmyndighet kan agera på rapporterna och det är PTS som i egenskap av expertmyndighet kan ge snabbt stöd till den som drabbats av en incident. PTS kan vidarebefordra rapporterna till CSIRT. Telenor har uppfattat att det från vissa håll finns tankar på att flytta CSIRT från MSB till det nationella cybersäkerhetscentret. Detta avstyrker Telenor med skärpa, men det visar på att MSB i egenskap av värd för CERT-SE inte nödvändigtvis behöver äga incidentrapporteringsföreskrifterna eller ta emot samtliga incidentrapporter

I tillägg till föreskrifter finns ett behov av vägledning och utbildning som är tillräckligt konkret för att verksamhetsutövarna ska kunna göra rätt från början. Tillsynsmyndigheter känner ibland ett motsatsförhållande till att både vara rådgivande och tillsynande, vilket Telenor anser vara olyckligt. Det bör därför uttryckligen anges i lagen och myndigheternas instruktioner att de har en rådgivande roll avseende cybersäkerhetslagens bestämmelser och att rådgivningen kan ske både genom att publicera vägledningar, erbjuda utbildningar och genom forum för dialog.

NIS och CER direktiven tar sikte på att stärka den inre marknaden och harmoniserad riskhantering och säkerhetsarbete ska i möjligaste mån ersätta nationell särreglering som verkar hämmande på den inre marknadens funktion. Telenor ser tyvärr hur Sverige reagerar på hot och omvärldshändelser genom att införa nationella säkerhets-bestämmelser som försvårar eller helt hindrar verksamhet över gränserna. Telenor är verksamt på fyra nordiska marknader men kan pga svenska särbestämmelser (5G-licenskrav och säkerhetsskyddslagen) inte samarbeta effektivt med andra nordiska verksamheter inom koncernen. Det är en utveckling som går emot både den europeiska ambitionen om en inre marknad och det nyligen ingångna NATO-medlemskapet. Regeringen bör skyndsamt göra en översyn av den svenska särregleringen och utvärdera om den i alla delar verkligen är motiverad av säkerhetsskäl.

Övrigt

Telenor står till regeringens förfogande om det finns behov av ytterligare upplysningar. Telenor åberopar inte sekretess för någon uppgift i detta remissvar.

Telenor Sverige AB

Martin Sjöberg
Bolagsjurist