Försvarsdepartementet

E-post: fo.remissvar@regeringskansliet.se

med kopia till visnja.raguz@regeringskansliet.se

Fö2024/00496

Stockholm 2024–05–27

Remissyttrande om delbetänkandet *Nya regler om cybersäkerhet (SOU 2024:18)*

Teracom Group AB (Teracom) har beretts tillfälle att yttra sig över rubricerat betänkande och önskar framhålla följande.

Sammanfattande kommentarer

Teracom anser att delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) (”Delbetänkandet”) innebär viktiga förslag för en förbättrad cybersäkerhet i Sverige, men att det krävs ytterligare överväganden och justeringar för att säkerställa att förslagen blir både effektiva och praktiskt genomförbara. Regleringar inom området cybersäkerhet kommer i all tätare följd och det är av stor vikt att dessa säkerställs hänga ihop. Kraven som ställs på verksamhetsutövare i en allt snabbare takt innebär att även kommunikation, införandetid och stöd införs i samma takt. Genom att adressera de ovan nämnda punkterna kan Sverige bättre rustas mot framtida cybersäkerhetshot.

Efter att tagit del av Delbetänkandet anser Teracom att det finns behov av en starkare nationell samordning gällande cybersäkerhetsåtgärder. Detta kan med fördel inkludera inrättandet av en central myndighet med övergripande ansvar för cybersäkerhet i Sverige, vilket torde underlätta ett enhetligt och koordinerat arbetssätt framgent. Det skulle även kunna ske via ett tilläggsuppdrag till Försvarets radioanstalt, FRA, som i så fall skulle vara ensamt ansvarig för ett sådant center.

Vidare ser Teracom en utmaning gällande samordning då flera olika utredningar sker parallellt. Som ett exempel uppfattar Teracom att de förslag som tidigare presenterats i delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning inte stämmer överens med det som föreslås i detta Delbetänkande.

Teracom AB
Lindhagensgatan 122
Box 30150
104 25 Stockholm
Tel 08-555 420 00
Org.nr. 556441-5098
www.teracom.se

Föreskrifter
I Delbetänkandet föreslås att varje tillsynsmyndighet inom sitt tillsynsområde får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap1–3 §§ lagen om cybersäkerhet. Teracom anser att det primära ansvaret för att meddela gemensamma grundföreskrifter för cybersäkerhetslagen i stället bör ligga hos en myndighet, men att tillsynsmyndigheterna ska ges möjlighet att meddela kompletterande sektoranpassade föreskrifter om det behövs.

Innehållet i föreskrifterna som, enligt utredningens förslag, de elva tillsynsmyndigheterna ska utfärda bedöms rimligen vara till stor del detsamma. Nyttan av en sådan ordning kan därför ifrågasättas. För det fall innehållet i dessa föreskrifter i stället skulle visa sig variera framstår en sådan ordning överraskande och, inte minst för verksamhetsutövare som tillhör flera olika sektorer, otydlig.

Att en myndighet ges det primära ansvaret att meddela gemensamma grundföreskrifter bör kunna gynna en tydlighet inom cybersäkerhetslagens tillämpningsområde. En sådan ordning skulle vidare säkerställa att verksamhetsutövare oavsett sektor tillämpar samma föreskrifter och därmed underlätta ett sektoröverbryggande erfarenhets- och lärandeutbyte, som enligt Teracom är eftersträvansvärt.

Incidentrapportering
Det är viktigt att underlätta incidentrapportering för verksamheter. En omfattande och diversifierad rapportering i olika mallar och format till olika myndigheter riskerar att, förutom att det tar tid och resurser från verksamheterna, leda till missnöje. Att i stället sträva efter att verksamheter författar en incidentrapport som alla inblandade myndigheter kan ta del av, vore att föredra.

För att få till en väl fungerande incidentrapportering är det troligtvis avgörande att verksamheterna förstår vikten av att lägga resurser på rapporteringen. En förutsättning för detta är att alla mottagare av rapporterna inte upplevs som anonyma. Det torde även vara relevant att lärdomar från olika incidenter kommer alla verksamheter till del, för att kunna ”lära av varandras misstag”. De senaste årens tendens att sekretessklassa i stort sett all information kring incidenter medför att lärandet uteblir.

Om sådan, mer öppen, reglering av sekretesskäl inte anses möjlig bör tillsynsmyndigheterna ges ett tydligt uppdrag att på ett anonymiserat sätt säkerställa att verksamhetsutövarna får del av lärdomar och information om incidenter från andra verksamhetsutövare.

Det är också av vikt att en incidentrapport hanteras som just en möjlighet till lärande. Om en anmälan om en incident automatiskt leder till tillsyn och stor risk för sanktioner, finns det risk att verksamheter antingen låter bli att rapportera incidenter eller utelämna viss information.

Tillsyn, ingripande och sanktioner
Enligt Delbetänkandet ska tillsynsmyndigheter inte ha möjlighet att ingripa med förelägganden och sanktioner mot verksamheter som inte följer kraven på systematiskt och riskbaserat informations- och cybersäkerhetsarbete.

Teracom anser att just ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete är grunden för en bra säkerhet. Att då undanta denna del för tillsynen sänder dels fel signaler, dels minskar det myndigheternas möjligheter att förebygga incidenter och säkerställa att verksamheterna gör grundarbetet.

Teracom anser därför att tillsynsmyndigheterna bör ha befogenhet att både ägna sig åt tillsyn och ingripa då verksamheter inte följer de krav som finns på systematiskt och riskbaserat informations- och cybersäkerhetsarbete.

Sanktionsavgifter
Teracom tillstyrkes utredningens förslag att strikt ansvar bör gälla för NIS2 och att sanktionsavgifter ska kunna utdömas även om överträdelser skett på grund av försummelse eller oaktsamhet. Detta är viktigt för att tvinga berörda verksamheter att ta sitt informationssäkerhetsansvar fullt ut.

Dock skulle det, när lagen träder i kraft, och om det inom NIS2 är möjligt, finnas en frist där sanktionsavgifter inte ges under en begränsad övergångstid vid eventuella överträdelser.

Övrigt
Teracom vill även tillägga att begreppen ”säkerhetsåtgärder” och ”riskhanteringsåtgärder” inte nödvändigtvis betyder exakt samma sak. Det är förvisso lämpligt att i så stor utsträckning som möjligt bibehålla inarbetad nomenklatur. Men när de i direktivet definierade faktorerna som ska beaktas har dubblerats i antal i den nya versionen, så finns det all anledning att uppmärksamma detta genom att använda den typen av formulering som nu föreslås i Delbetänkandet – och som samtidigt är mer överensstämmande med den nomenklatur som används i standarder för ledningssystem. Teracom delar således utredningens förslag i dessa delar.

_____

Åsa Sundberg
Vd och koncernchef
Teracom

Johan Grufman
IT Säkerhetschef
Teracom