Datum
2022-01-10

Er referens
Fö2021/00796
Vår referens
-

TechSverige

Försvarsdepartementet

fo.remissvar@regeringskansliet.se

Remissvar avseende betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

TechSverige har beretts tillfälle att lämna remissvar över rubricerat betänkande (dnr Fö2021/00796). TechSverige (tidigare IT&Telekomföretagen) är en bransch- och arbetsgivarorganisation för företag inom techsektorn med drygt 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i förbundsgruppen Almega och därmed i Svenskt Näringsliv.

TechSverige välkomnar fortsatt arbete inom informations- och cybersäkerhet, men påminner om sitt tidigare lämnade remissvar (1 april 2019) avseende betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:585) där TechSverige ställde sig bakom Svenskt Näringslivs remissvar och framförde några ytterligare synpunkter, vilka i korthet var

- problemen med företag som blir indirekt berörda av lagstiftningen
- osäkerheten kring bland annat egendomsskyddet, näringsfriheten och rätten till ersättning för åtgärder samt risken för att reglerna kan skada svenska företags konkurrenskraft
- att företagens självidentifiering är fortsatt tveksam – tillsynsmyndigheterna bör få i uppdrag att informera berörda företag och medel att ersätta dem som träffas av lagen
- att lagen medger rimlighetsbedömningar som ger möjligheter till undantag för små företag.

Nedan lämnar TechSverige synpunkter på några av förslagen och bedömningarna i det nu remitterade betänkandet.

Digitalisering och informations- och cybersäkerhet

Utredarens bedömning: *Digitaliseringen i samhället sker snabbt och i stor omfattning inom de flesta samhällssektorer. Digitalisering medför nya arbetssätt, som bygger på nya tekniska möjligheter att samla in stora mängder data. Förändringsfaktorer, bland annat utvecklingen av ny teknik, medför att nya sårbarheter och risker uppstår. Informations- och cybersäkerhet i samhället i stort och inom olika samhällsviktiga områden utvecklas inte i motsvarande grad vilket innebär att gapet mellan digitalisering och informations- och cybersäkerhet ökar över tiden. Detta medför även ökade risker för cyberangrepp mot eller it-incidenter i säkerhetskänsliga och andra samhällsviktiga verksamheter.*

TechSverige delar i stort utredarens bedömning.

TechSverige välkomnar regeringens fortsatta arbete med att stärka informations- och cybersäkerhet i Sverige. God säkerhet är en förutsättning för att maximera möjligheterna med digitaliseringen och för att skapa förtroende för den digitala utvecklingen i samhället, hos företag och individer. Olika typer av hot och sårbarheter behöver hanteras för att värna verksamhets- och affärsnytta, personlig integritet, tillit och trygghet.

Hoten mot våra IT-system förändras och blir alltmer asymmetriska. I dag är allt och alla potentiella måltavlor och vem som helst kan med små medel utföra angrepp som kan ge stora konsekvenser. Vi måste därför kunna hantera helheten och detaljerna på samma gång; förstå interna och externa hot, fysisk och logisk säkerhet, risken att utnyttjas som verktyg i attacker mot andra och beakta den mänskliga faktorn. Detta ger ett kraftigt ökat behov av insikt, mognad och kompetens hos såväl beställare som leverantörer.

Det är välkommet med ytterligare samordning mellan statliga myndigheter. I ett branschperspektiv är det angeläget att både Post- och telestyrelsen (PTS) och Myndigheten för samhällsskydd och beredskap (MSB) har en tydlig plats i det.

Det finns också möjligheter att ytterligare utveckla arbetet med hur staten involverar privata aktörer i säkerhets- och totalförsvarsarbetet (i ett bredare perspektiv än vad som har varit utredarens uppdrag).

Uppdraget till FMV

Utredarens förslag: *Regeringen ska ge Försvarets materielverk (FMV) i uppdrag att i samråd med övriga myndigheter som ingår i det nationella cybersäkerhetscentret och övriga tillsynsmyndigheter inom säkerhetsskyddsområdet att fortsätta arbetet med bland annat analyser och lämna förslag.*

TechSverige kommenterar förslaget.

För all standardisering och certifiering är det viktigt att det råder öppenhet i processerna och att restriktioner grundas på objektiva kriterier. Vidare krävs stor förståelse för hur kommersiell verksamhet bedrivs, som till exempel nät för elektronisk kommunikation eller andra säkerhetskänsliga system.

TechSverige har ingen annan uppfattning än utredaren om att FMV besitter kompetens inom själva sakområdet. Det är dock viktigt att beakta detta, och andra relaterade frågor, i ett längre tidsperspektiv.

I ett snart sagt genomdigitaliserat samhälle som Sverige behöver de offentliga aktörerna åtnjuta ett högt förtroende och ha goda möjligheter att samarbeta med den privata sektorn. I betänkandet och i diskussionerna kring Sveriges säkerhet, informations- och cybersäkerhet med mera ges försvars-, säkerhets- och polismyndigheter ofta en framträdande roll. Utredarens förslag att ge FMV uppdraget grundar sig främst på dagens situation och FMV:s kompetens i dagsläget. TechSverige anser att regeringen bör pröva frågan i ett vidare perspektiv och se till hela fältet säkerhet, informations- och cybersäkerhet när ansvaret fördelas.

Utan att värdera andra myndigheters förmåga och bidrag på området konstaterar TechSverige att MSB har ett bredare uppdrag och oftare riktar sig till många intressenter i samhället, inklusive företag. Vår uppfattning är att det långsiktigt vore lämpligare att förstärka MSB:s uppdrag, utöka myndighetens kontaktytor mot näringslivet och samla fler frågor om informations- och cybersäkerhet hos myndigheten.

Nationell anpassad certifieringsordning

Utredarens bedömning*: Det för närvarande inte finns tillräckliga skäl att införa en nationell särskilt anpassad ordning med krav på certifiering av IKT-produkter, IKT-tjänster och IKT-processer som används i säkerhetskänslig verksamhet.*

TechSverige har inga invändningar mot bedömningen.

TechSverige utgår ifrån att regeringen eller ansvariga myndigheter hämtar in synpunkter från näringslivet innan denna eller liknande åtgärder föreslås längre fram i tiden.

Rätt till tillgång till informationssystem

Utredarens förslag: *I säkerhetsskyddslagen införs en ny bestämmelse med innebörden att tillsynsmyndigheten ska, i den omfattning som det behövs för tillsynen, ha rätt att få tillgång till informationssystem som används i verksamhet som omfattas av tillsyn. Tillsynsmyndigheten ska även få besluta att förelägga den som står under tillsyn att ge tillgång till sådana informationssystem samt ha möjlighet att förena föreläggandet med vite.*

TechSverige avstyrker förslaget.

Förslaget bör inte genomföras i sin nuvarande form. Det säkerhetsarbete som bedrivs mellan privata och offentliga aktörer måste ske med högt förtroende och hög tillit. Lagar och regler, liksom andra åtgärder bör ha detta som utgångspunkt. Vidare måste det vara höga krav på både rättssäkerhet och förutsägbarhet.

Arbetet med informations- och cybersäkerhet ställer stora krav på kunskap om hur till exempel elektroniska kommunikationsnät eller annan säkerhetskänslig verksamhet bedrivs i kommersiella sammanhang. Det är inte rimligt att anta att vare sig Säkerhetspolisen eller Försvarsmakten kan ha eller upprätthålla sådan kunskap på hög nivå.

Föreliggande förslag är ingripande och presenteras inte på ett sätt som ökar förtroendet. Till exempel beskriver betänkandet knappast alls riskerna med förslaget. Vidare bör tillsynsmyndigheternas befogenheter enligt den nyligen införda lagstiftningen först utvärderas innan befogenheterna utökas.

Konsekvenserna av förslaget är heller inte nöjaktigt utredda. TechSverige notera att diskussionen om skyddet av den enskildes integritet är förvånansvärt kort och rimligen ofullständigt (s. 473). Det gäller också frågor om företagshemligheter och börspåverkande information med mera. I avsnittet om konsekvenser gör utredaren gällande att kostnaderna för att bistå tillsynsmyndigheten som regel bör vara begränsade utan att närmare underbygga det. Detta står i stark kontrast till uppfattningen att staten bör ersätta verksamhetsutövares kostnader som går utöver vad som kommersiellt kan försvaras (se punkterna om tidigare kritik i inledningen).

Skulle, trots ovan argument, en sådan regel ändå införas bör den omformuleras så att rätten till tillgång blir ett undantag vid till exempel särskilda behov i stället för betänkandets formulering ”i den omfattning som det behövs för tillsynen”.

Lämplighetsprövning av driftsättning av informationssystem

Utredarens förslag: *Det införs krav på verksamhetsutövaren att pröva om en driftsättning av ett informationssystem i säkerhetskänslig verksamhet, eller en väsentlig förändring av systemet, är lämplig ur säkerhetsskyddssynpunkt. Om det leder till bedömningen att det förfarandet är olämpligt från säkerhetsskyddssynpunkt får det inte inledas.*

Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren i vissa fall samråda med samrådsmyndigheten (Säkerhetspolisen eller Försvarsmakten).

Även samrådsmyndigheten kan initiera samråd och besluta om åtgärdsföreläggande mot verksamhetsutövaren. Om ett föreläggande inte följs eller om det förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, får samrådsmyndigheten förbjuda driftsättningen eller förändringen av informationssystemet.

TechSverige avstyrker förslaget.

Att samrådsmyndigheten får besluta om åtgärdsföreläggande och förbjuda driftsättningen är ingripande och bör inte genomföras på det sätt som utredaren föreslår.

TechSverige och andra har framfört att den nu gällande lagen innehåller otydligheter och osäkerhet. Det här föreslagna samrådsförfarandet minskar inte otydligheten och osäkerheten för verksamhetsutövarna.

Med både en tillsynsmyndighet och en samrådsmyndighet (för en given verksamhetsutövare) finns det risk för en oklar ansvarsfördelning, till nackdel för både myndigheter och berörda företag, liksom dubbelarbete och ineffektiv tillsyn. En ordning där samrådsmyndigheterna stöder tillsynsmyndigheterna med informationssäkerhetskompetens bör i stället övervägas.

För verksamhetsutövaren kan det bli krångligt eller till och med riskfyllt att till exempel uppdatera (om det anses vara en väsentlig förändring) eller byta system. Detta kan onödigt försena nyttiga och viktiga förändringar i ett informationssystem. Förmodligen är det i många fall också svårt för samrådsmyndigheten att fullt ut förstå och förutse konsekvenserna av ett åtgärdsföreläggande.

Ett beslut om åtgärdsföreläggande och förbud måste vara proportionerliga mot de praktiska konsekvenser, eventuell skada samt de risker och hot som kan uppkomma om ett informationssystem inte kan används vid en viss tidpunkt. Följaktligen ställer utredarens förslag mycket stora krav på att samrådsmyndighetens arbete kan utföras i god tid, med hög kompetens liksom med en god förståelse för möjliga konsekvenser av fattade beslut.

Det finns vidare en risk att samrådsmyndigheten fattar ett beslut som till viss del beror på tidsbrist eller andra brister i myndighetens eget arbete – snarare än en faktisk bedömning av system och konsekvenser. Kort sagt – det kan vara bekvämare att fälla än att fria för att minimera riskerna för samrådsmyndigheten själv.

Tillgången på personal med kompetens inom informations- och cybersäkerhet måste öka

Utredarens bedömning*: Det finns i dag ett omfattande behov av personal med kompetens i informations- och cybersäkerhet på olika nivåer hos många verksamhetsutövare, såväl inom den offentliga verksamheten som i näringslivet. Tillgången på personal med kompetens inom informations- och cybersäkerhet behöver därför öka.*

TechSverige delar utredarens bedömning att det finns omfattande behov av personal med kompetens i informations- och cybersäkerhet.

Lagstiftningsförslag och många andra åtgärder för att öka informationssäkerheten blir svåra att genomföra och kommer inte att få önskade resultat om inte rätt kompetens finns tillgänglig. Givet statens starka roll avseende styrning av och resurser till utbildning hade det varit önskvärt att utredaren var mer utförlig i sin analys och lämnade fler förslag för att stärka kompetensförsörjningen inom informations- och cybersäkerhet.

TechSverige anser att regeringen snabbt bör vidta fler åtgärder för att stärka kompetensförsörjningen inom informations- och cybersäkerhet.

FÖR TECHSVERIGE

Christina Ramm-Ericsson
Näringspolitisk chef

Fredrik Sand
Näringspolitisk expert