Försvarsdepartementet

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

# Remissvar avseende delbetänkande Nya regler om cybersäkerhet (SOU 2024:18)

TechSverige har beretts tillfälle att lämna ett remissvar avseende rubricerat delbetänkande (dnr Fö2024/00496).

TechSverige 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 Svenskt Näringsliv.

# Inledning

Ett antal nya regelverk inom datarätt, digitalisering, AI och cybersäkerhet ger företag en stor regel- och kostnadsbörda att hantera. TechSverige noterar att den omfattande regleringsvågen starkt påverkar företagens kostnadsläge, innovation och konkurrenskraft. Verksamhet och investeringar skjuts upp tills företagen hunnit överblicka, förstå och finansiera den nya regelbördan. När de nya reglerna består av direktiv är det av stor vikt att genomförandet i Sverige ger företag verksamma här den bästa möjliga lagstiftningen utan att reglera mer än vad som ansetts proportionerligt och lämpligt inom övriga EU. Därför utgår vi ifrån att regeringens uppdrag till utredningen att förslagen ska utformas så att regelbördan och administrationen minimeras respekteras och säkerställs av lagstiftaren.

Det är därför med oro och beklagande TechSverige noterar att man i utredningen ändå väljer att lägga förslag som går längre än vad direktivet anger och utan att närmare analysera behovet och nyttan i förhållande till kostnaden av dessa. Detta står också i stark kontrast till det uppdrag utredningen fått ”Om förslag lämnas som går utöver EU-direktivens krav, ska utredaren särskilt motivera varför dessa är nödvändiga för att uppnå nationella svenska mål och göra en analys av om förslagen är samhällsekonomiskt effektiva och hur förslagen påverkar svenska företags konkurrenskraft.[1]

Exempel på sådana extra krav är bl.a. kravet på cybersäkerhetsutbildning där det i direktivet står att verksamheterna ska uppmuntras att erbjuda sådan utbildning, medan utredningen föreslår ett krav att alla ska erbjudas utbildning. Vidare föreslår utredningen att det personliga ansvaret för att uppfylla skyldigheterna i lagen ska åläggas enskilda styrelseledamöter. Detta är inte något som följer av direktivet och en styrelse fattar sina beslut kollektivt. Kravet på säkerhetsrevision (på tillsynsobjektets bekostnad) har heller inte sin grund i direktivet. Vad som skulle kunna uppfattas som en mindre skillnad blir i praktiken en reell skillnad, är att utredningen föreslår att verksamheterna ska utföra ett systematiskt säkerhetsarbete medan direktivet kräver ett riskbaserat arbete. Samtliga dessa exempel på genomförande utöver direktivet riskerar att ge företag verksamma i Sverige högre

[1] Dir. 2023:30, s. 20.

kostnader för regelefterlevnad än företag i andra medlemsstater, vilket naturligtvis påverkar svenska företags konkurrenskraft på den inre marknaden.

Att samarbeta och dela kunskap är avgörande för att stärka vår gemensamma cybersäkerhet. Privat-offentligt samarbete utgör en mycket viktig del i cybersäkerhetsarbetet för att förhindra, hantera och följa upp och dra erfarenheter. Betänkandet tar dock inte upp denna aspekt, vilket är beklagligt. Ett närmare samarbete mellan tillsynsmyndigheter och företag inom de sektorer som omfattas av reglerna bör prioriteras. Dessutom är det nödvändigt att ge stöd och vägledning till de verksamheter som tidigare inte har varit föremål för NIS-reglerna, särskilt små och medelstora företag.

Mot bakgrund av det stora behovet av stöd och vägledning blir det också viktigt att behöriga myndigheter samarbetar för att säkerställa en enhetlig tolkning, tillämpning och undvika oklarheter för företagen. Det blir särskilt viktigt när företag står under tillsyn av flera myndigheter.

# Statlig ansvarsfördelning avseende informations- och cybersäkerhet

TechSverige presenterade en rapport om informations- och cybersäkerhet 2023.[2] Några viktiga budskap i rapporten var att

- det behövs en marknadsledd utveckling för att hantera frågorna
- ingen enskild aktör kan lösa problemen inom informations- och cybersäkerhet – det ställer stora krav på ansvarsfördelning och samarbete, inte minst mellan privat och offentlig sektor
- kompetensbristen – i Sverige och i EU – hotar informationssäkerheten och här kan det offentliga lämna sitt största bidrag – åtgärder för att minska bristen.

En annan strategisk fråga som berör det remitterade delbetänkandet är ansvarsfördelningen inom informations- och cybersäkerhet mellan statliga myndigheter.

En stor del av ansvaret är redan fördelat genom både svensk och europeisk lagstiftning. Annat följer av andra internationella förhållanden. Det finns tillsynsmyndigheter som har uppdrag inom informations- och cybersäkerhet, liksom beredskaps- och sektorsmyndigheter för områden där användningen av it och säkerhet kommer att ha betydelse för de verksamheter som ska bedrivas. Frågorna kommer också att aktualiseras inom ramen för den nya struktur som etablerats inom civilt försvar med civilområdesansvariga länsstyrelser som antagligen kommer att behöva hantera frågor om t.ex. it-beroenden.

Informations- och cybersäkerhetsarbetet sker på allt från en teknisk nivå, via standarder, organisationer och myndigheter till en nivå med policy i Sverige, inom EU eller andra internationella forum. Det är många lager, många professioner etc. med olika uppdrag och befogenheter som är inblandande. Ingen aktör bör, eller kan för den delen, ta helhetsansvaret. Hittills har diskussionen i Sverige handlat mer om *vem* som ska göra något i stället för *vad* som ska göras och hur ser i så fall en lämplig ansvarsfördelning ut.

Frågorna har kretsat kring de myndigheter som ingår i Nationellt cybersäkerhetscenter (NCSC), med fokus kanske främst på deras uppdrag avseende underrättelsetjänst, säkerhetstjänst och brottsbekämpande uppgifter. Dessa myndigheter har viktig teknisk kompetens eller har tillgång till uppgifter som kan vara avgörande för ett framgångsrikt systematiskt arbete med informations- och cybersäkerhet eller inför hot och under incidenter. Är utmaningen den hur staten ska organisera sig kring den mer snäva synen på t.ex. underrättelser eller är det bredare informations- och cybersäkerhetsfrågor i hela samhället som ska styra hur ansvaret ska fördelas?

[2] Techbranschens förslag för att möte cyberhoten, <https://www.techsverige.se/37801-2/>.

I många fall är det driftsäkerhet och den verksamhet som utförs (med hjälp av it-system) som är det avgörande (som NIS2-direktivet också är ett uttryck för), och kanske inte främst sekretess, brottsbekämpning, skydd mot underrättelseinhämtning m.m.

Ett annat sätt att närma sig frågorna skulle kunna vara att det är de verksamheter som ska kunna fungera, deras sammanhang samt det ansvar och de regelverk som redan finns eller utvecklas som det remitterade delbetänkandet om NIS2, cyberresiliensakten (CRA) m.fl.som ska vara i fokus.

Centrala underrättelse- och säkerhetsmyndigheter har mycket att bidra med, men har också begränsningar i uppdrag, förmåga, resurser m.m. för att förstå hur it-system och hoten mot dem samspelar ute i organisationer, i processer och med regelverk på flera olika nivåer. Där kan myndigheter närmare verksamheter och företag ha avgörande insikter. Genom åren har nog denna fråga underskattats – hur och var olika myndigheter bäst bidrar i systemet.

Den strategiska frågan blir då hur staten ska samordna ett ganska stort antal myndigheter, i olika sektorer, med olika rättsliga förutsättningar och där t.ex. teknikkompetens och underrättelser kanske inte ens är den avgörande frågan sett över tid och för att den lägsta nivån av informations- och cybersäkerhet i Sverige ska kunna höjas.

Att vardaglig verksamhet inom it-beroende verksamheter knyts närmare till underrättelse- och säkerhetstjänster kan väcka frågor i det internationella samarbetet och principiellt. Dessa myndigheter har också stora behov av sekretess och skydd av metoder som gör det svårare för dem att ansvara för att nå långt ut i samhället. Deras kärnuppdrag är viktiga men kanske också begränsar förmågan att hantera informationssäkerhetsarbetet brett och i skilda sektorer med olika regelverk. Här måste myndigheter med marknadskännedom, tillsynsuppdrag m.fl. involveras som positiva krafter för att höja säkerheten. Det är förstås av strategisk vikt att staten förmår organisera sig på ändamålsenligt sätt.

Det finns även andra strategiska frågor. Det är viktigt att ansvariga myndigheter har god förståelse för kommersiella realiteter inom olika sektorer och att de har konkurrens- och tillväxtfrågor i åtanke. Företag vill ogärna ha flera myndigheter som utövar tillsyn eller uppställer rapporteringskrav. I några fall kan staten själv ha strategiska intressen av en god ordning för informationsutbyte, då företag i många fall kan ha bättre information än statliga myndigheter.

I andra fall måste ett ansvar inom informations- och cybersäkerhet också kombineras med djup förståelse för de verksamheter som berörs, som t.ex. energiförsörjning, vård och transporter. Vidare behöver detta också ske på ett sådant sätt att statliga myndigheter med informationssäkerhets- och cybersäkerhetkompetens inte konkurrerar med privata aktörer och att företag inte i onödan och ofta drabbas av ingripande åtgärder eller administrativa bördor och kostnader.

I föreliggande delbetänkandet lämnas förslag baserade på NIS2-direktivet som kommer att påverka arbetet och ansvarsfördelningen under lång tid. TechSverige har tidigare på eget initiativ lämnat ett remissvar avseende Ett nytt Nationellt cybersäkerhetscenter – del 1 (dnr Fö2024/00785). Där avstyrkte TechSverige huvudförslagen. Några av dem behandlas också i föreliggande delbetänkande.

* * *

Nedan lämnar TechSverige några övergripande synpunkter liksom några mer konkreta synpunkter på förslagen i det remitterade delbetänkandet.

# Övergripande synpunkter

**TechSverige anser att lagstiftaren ska hålla sig till intentionerna med direktivet.**

Syftet för den föreslagna lagen behöver förtydligas. Det är inte tydligt om lagen har samma syfte som direktivet: att med cybersäkerhet främja den inre marknaden – eller om lagen också avser att bemöta en hotbild som omfattar fredstida kris och krig, dvs. höjd beredskap. Inom det området pågår annat arbete och skulle rimligen ställa andra krav på t.ex. konsekvensbeskrivningarna i betänkandet.

Lagstiftaren i Sverige har tidigare kritiserats för att inte se till syftet med nya EU-regler när de införs i Sverige. Det underliggande NIS2-direktivet är en inremarknadsreglering från EU. Genomförandet i Sverige bör hålla sig till direktivets syfte och inte utsträckas till att omfatta andra områden som inte är avsedda att regleras som en inremarknadsfråga.

Samtidigt är det uppenbart att NIS2-direktivet och dess genomförande ligger nära och påminner om det arbete som görs för totalförsvarsfrågor som t.ex. höjd beredskap. Det finns därför möjlighet att organisera det arbetet och t.ex. den statliga ansvarsfördelningen inom området som underlättar för dem som omfattas av NIS2-direktivet – utan att själva syftet med direktivet förfelas.

## Myndigheten för samhällsskydd och beredskaps roll

**TechSverige tillstyrker förslaget att Myndigheten för samhällsskydd och beredskap (MSB) fortsatt utgör gemensam kontaktpunkt, CSIRT-enhet och får den nya rollen som nationell cyberkrishanteringsmyndighet.**

Att MSB får dessa roller bör rimligen få konsekvenser för andra delar av ansvarsfördelningen inom informations- och cybersäkerhet. Regeringen har aviserat en ny nationell strategi för informations- och cybersäkerhet. Regeringen har också remitterat Ett nytt Nationellt cybersäkerhetscenter (Fö2024/00785) som lämnar förslag inom området som TechSverige avstyrker. Politiken på området skulle vinna på mer samordning.

Det är rimligt att MSB blir cyberkrishanteringsmyndighet då konsekvenser av en cyberkris ofta är att en verksamhet eller tjänst inte kan utföras. Det som ska hanteras är inte bara it-systemen, utan också att verksamheten störs och konsekvenserna av det. Här har MSB en central roll och erfarenhet av att samverka med tillsyns-, beredskaps- och sektorsmyndigheter och bättre förutsättningar att hantera helheten.

**TechSverige föreslår att utgångspunkten för ansvarsfördelningen bör vara förslagen i delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18).**

Förslagen baseras på EU-regler som rimligen är svårare för lagstiftaren att direkt påverka och kommer därför att bli beständigare. Vidare har den aktuella utredningen genomfört ett mer gediget arbete än den om NCSC som har haft kort tid på sig.

Som framgått ovan anser TechSverige att NIS2-direktivets genomförande ska hålla sig till direktivets syfte. Det är dock rimligt att anta att den struktur som nu etableras kommer att påverka en rationell och effektiv utformning av ansvarsfördelningen mellan myndigheterna i totalförsvarsarbetet och liknande frågor.

Att nu flytta Nationellt cybersäkerhetscenter (NCSC) till Försvarets radioanstalt (FRA) framstår som mindre önskvärt än att hålla NIS2-rollerna samlade hos MSB. Snarare skulle NCSC föras till MSB. Det går också att tänka sig att en ny myndighet, inriktad på det breda informationssäkerhetsarbetet i samhället (som NIS2-direktivet är ett uttryck för), är en annan möjlig väg fram.

Att FRA eller andra polis-, säkerhets-, försvars- eller underättelsemyndigheter som har varit tongivande i NCSC-samarbetet skulle vara särskilt lämpande att nå ut i det vardagliga informationssäkerhetsarbetet i linje med NIS2-direktivet framstår i alla fall inte som uppenbart. Däremot har dessa myndigheter teknisk kompetens, information och under-

rättelser som behöver kunna utnyttjas även i det mer breda och vardagliga informationssäkerhetsarbetet och givetvis i dessa myndigheters huvuduppdrag.

**TechSverige anser att ytterligare utredningsarbete behövs för att utveckla ansvarsfördelningen inom informations- och cybersäkerhet.**

Det är tydligt att tidigare åtgärder inte har resulterat i en ändamålsenlig ansvarsfördelningen inom informations- och cybersäkerhetsarbetet. I väntan på en nationell strategi och med flera förslag som förväntas genomföras inom kort riskerar situationen att försämras på kort och medellång sikt.

Det vilar ett stort ansvar på den här regeringen att inte bara vidta åtgärder snabbt – utan också genomtänkt. Därför bör förslagen i det remitterade delbetänkandet (i stort) genomföras och bli utgångspunkten för det fortsatta arbetet med informationssäkerhet brett i samhället.

## Post- och telestyrelsen som tillsynsmyndighet

**TechSverige tillstyrker att Post- och telestyrelsen (PTS) ska vara tillsynsmyndighet för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster samt rymden.**

PTS är sedan enligt NIS-reglerna tidigare tillsynsmyndighet för digital infrastruktur samt för digitala tjänster.[3] TechSverige ser det som en fördel att liknande, tillkommande sektorer samlas under samma tillsynsmyndighet.

## Behåll möjligheten att avstå från att besluta om sanktionsavgifter

**TechSverige anser att det är angeläget att det finns flexibilitet när det gäller att besluta om sanktionsavgifter.**

Sanktionsavgifter i många EU-regler innebär ofta att det beslutas om höga belopp i tillsynsarbetet grundat på omständigheter som kan vara svåra att tillfullo genomlysa. Sanktionsavgifter bör följaktligen användas med försiktighet och det är angeläget att tillsynsmyndigheterna i varje enskilt fall kan avgöra om sanktionsavgift överhuvudtaget ska tas ut – alltså inte att beslut om sanktionsavgifter ska fattas undantagslöst vid konstaterad överträdelse.

## Bristande konsekvensanalys

TechSverige instämmer i Regelrådets yttrande att redovisning avseende påverkan på företag är bristfällig. Det saknas helt analys av de ekonomiska effekterna på företag som kommer omfattas av förslaget, vilket inte kan ses som annat än att utredningen inte har uppfyllt sitt uppdrag enligt konsekvensutredningsförordningen (2007:1244).

[3] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

# Närmare om betänkandet och förslagen

## 1.1 Förslag till lag om cybersäkerhet

**TechSverige anser möjligheten att inte informera användare om hot ska finnas kvar – för de fall där det inte är lämpligt.**

Av direktivet framgår det att kravet på att informera gäller att informera användare om eventuella åtgärder som de kan vidta. Vidare ska information om ett hot endast ske "när så är lämpligt". I vissa situationer kan det vara olämpligt att informera om ett hot och därför bör informationen i sådana fall endast innehålla förslag på åtgärder, det bör återspeglas i det svenska genomförandet.

**TechSverige anser att säkerhetsskanningar ska omfattas av begränsningar.**

Förslaget till lag innebär att tillsynsmyndigheter ska kunna göra säkerhetsskanningar hos verksamhetsutövare. Det sägs inte något närmare om vilka begränsningar skanningarna ska ha, hur de ska utföras eller var de får utföras. Sådana skanningar är mycket ingripande åtgärder och måste alltid ske i samarbete med verksamhetsutövaren och med tydliga kriterier om när de får genomföras. Hur resultaten hanteras måste också regleras, då de kan innehålla säkerhetskänslig information.

## 4.5 Digital infrastruktur

**TechSverige anser att en restriktiv tolkning av begreppet leverantör av DNS-tjänst bör användas.**

Företag och andra organisationer kan ha DNS-servrar som endast används i den egna verksamheten (domäner). Det borde rimligen falla utanför syftet med direktivet och därför undantas.

## 5.2.2 Verksamhetsutövare

**Enligt TechSverige bör lagstiftaren noga överväga konsekvenserna av tillämpningen av lagen avseende verksamhetsutövare, i de fall då verksamhetsutövarna tillhandahåller tjänster som klassificeras som både väsentliga och viktiga, alternativt ryms i olika sektorer.**

Företag kan hamna under tillsyn av flera myndigheter. Tillsynen m.m. ställer stora krav på samordning av och mellan tillsynsmyndigheterna. Tillsynen kan bli ingripande och ofta ske för samma företag eller organisation om de utför flera tjänster som faller under direktivet. Det går också att tänka sig tjänster som ett företag tillhandahåller som inte faller under direktivet, och i de fall det står under tillsyn, vilken myndighet som då har ansvar. Tillsynsmyndigheterna bör följaktligen noga planera och samordna sin tillsynsverksamhet – även utanför NIS2-direktivets område.

Det måste fortsatt vara möjligt att använda olika nivåer av säkerhet inom samma verksamhetsutövare. Det kan t.ex. gälla administrativa system som inte direkt påverkar säkerheten i den reglerade tjänsten. Utan den möjligheten kan åtgärderna bli kostsamma och kontraproduktiva.

# 7 Riskhantering och incidentrapportering

**Enligt TechSverige bör PTS möjlighet att meddela undantag från skyldigheten att vidta säkerhetsåtgärder och att rapportera incidenter enligt lagen om elektronisk kommunikation kvarstå (LEK).**

PTS kan genom föreskrift besluta om undantag från skyldigheten att vidta säkerhetsåtgärder och skyldigheten att rapportera incidenter till tillsynsmyndigheten. Möjligheten behövs för att få bättre proportionalitetsbedömningar av enskilda åtgärder och bör finnas även i den nya lagstiftningen.

## 7.1 Övergripande lagreglering om riskhanteringsåtgärder

**TechSverige anser att PTS fortsatt ska vara den tillsynsmyndighet som har befogenhet att föreskriva om riskhanteringsåtgärder och ett riskbaserat informationssäkerhetsarbete.**

Allmänt sett, och där det är möjligt, är det förstås önskvärt att regler och föreskrifter är så lika som möjligt. Det är dock förmodligen svårt att i praktiken undvika regler som återspeglar förhållanden – och annan lagstiftning – som är speciella för de olika sektorerna.

PTS är den etablerade aktören och förmodligen den mest lämpande myndigheten att bedöma vad som kan vara ändamålsenligt både för det som har fallit under lagen om elektronisk kommunikation och även de tillkommande sektorerna. Därmed är det inte sagt att MSB inte kan bidra med vägledning och kunskap i det fortsatta arbetet.

Om det är möjligt, är gemensamma grundläggande krav att föredra och möjligen också i vissa fall lättare att ta fram för de tillkommande sektorerna. Det bör närmare analyseras hur sådana regler kan tas fram, inklusive vilka samråd och eventuella undantag som kan behövas. Som har noterats ovan, innebär genomförandet av NIS2 stora krav på statens förmåga att samordna myndigheternas arbete.

## 7.3 Incidentrapportering

**Incidentrapportering till följd av EU-regler är ett växande område. TechSverige anser att regeringen och lagstiftaren bör bedriva ett arbete för att förenkla för företagen som ska rapportera incidenter.**

Om det inte är möjligt att ha en central rapporteringsmekanism (för flera rapporteringskrav en s.k. one stop shop-lösning) bör varje företag rapportera till så få myndigheter som möjligt och helst endast till den närmast ansvariga tillsynsmyndigheten.

För att stärka den inre marknadens funktion och minska företagens administration är det centralt att incidentrapportering hanteras på samma sätt i medlemsstaterna. Här skulle en gemensam EU-mall vara att föredra och rapportering bör alltid kunna ske på engelska för att vara användbar inom hela EU. Dessutom bör ett förenklingsarbete påbörjas för att samordna och effektivisera incidentrapporteringskraven i olika lagstiftningar som t.ex. GDPR och kommande cyberresiliensakten.

Rapporteringsskyldigheterna föreslås bli mer långtgående än tidigare. Nytt är att även tillbud och cyberhot som kan orsaka en allvarlig driftsstörning ska rapporteras. Skyldigheten att rapportera potentiella framtida händelser verkar orimlig. Inrapportering av tillbud är oproportionerlig när man ser till administrativ börda. Det är också långt ifrån klart när ett hot blir betydande. Detta ökar företagens omotiverade rapporteringsbörda och kommer att vara rättsosäkert att tillämpa i praktiken.

Skyddet av företagens uppgifter och företagshemligheter behöver garanteras vid incidentrapportering med sekretess för att inte hämma incidentrapporteringen och öka antagonistiska angrepp.

## 9.6.3 Hinder mot att ta ut sanktionsavgift

**TechSverige anser att det inte ska vara tillåtet att utsättas för flera sanktionsavgifter för samma överträdelse. Det finns behov av att se över nivåerna på avgifterna.**

Möjligheten att ta ut sanktionsavgifter för personuppgiftsincidenter regleras både i NIS2-direktivet och i LEK. I dag kan även IMY besluta om sådana avgifter. Genomförandet av NIS2-direktivet och följdändringar bör säkerställa att det blir tydligt att sanktionsavgifter endast kan tas ut en gång för samma överträdelse. Nivåerna på avgifterna bör också samordnas – mot den lägre nivån.

## 11.2.9 Informera om betydande cyberhot

**TechSverige anser att reglerna om kraven på att informera kunder om cyberhot bör förtydligas.**

Både i den föreslagna cybersäkerhetslagen och i LEK finns krav på att informera kunder som kan antas påverkas av betydande cyberhot inom en viss angiven tid. Det finns behov av att förtydliga vad som ska gälla kring sanktionsmöjligheter vid information till användare om betydande cyberhot.

Det bör bara finnas en skyldighet att informera om betydande tillbud och hot när dessa är väsentliga och konkreta och verksamhetsutövaren på ett vederhäftigt sätt har kunnat bedöma allvarligheten. En vidare informationsskyldighet än så skulle riskera medföra spridning av rena spekulationer, och detta skulle kunna vara mycket skadligt utan att göra någon nytta.

Enligt förslaget ska verksamhetsutövaren informera kunder som kan antas påverkas av den betydande incidenten, och detsamma gäller betydande cyberhot (se 3 kap 6§). Värdet av information om en incident som kan få allvarliga konsekvenser är mycket begränsad. I de fall information om en betydande incident eller hot utgör eller kan komma att utgöra insiderinformation tillkommer ytterligare komplexitet, då bedömningar i den delen kräver viss konkretion. Spridning av information om eventualiteter kan leda till olämplig spridning av information som kan utgöra en säkerhetsrisk. Dessutom kan spridandet av sådan osäker information leda till spekulationer som (felaktigt) kan leda till oro på börsen.

## Kommentarer på valda paragrafer

För att ge exempel på några konsekvenser som de nya reglerna för cybersäkerhet kan komma att ha på företag lyfter TechSverige nedan fram några paragrafer och kommenterar dem

***3 kap. 3 §*** *Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.*

**Kommentar**: ”Ledningen” är inte definierat.

***5 kap. 8 §*** *Om ett föreläggande enligt 6 § inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos allmän förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).*

**Kommentar**: Förslaget ger tillsynsmyndigheten rätt att ingripa mot enskilda personer i verksamhetsutövarens ledning så inte bara mot organisationen utan även mot enskild person i ledningen.

***4 kap. 3 §*** *Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att denna lag eller föreskrifter som meddelats i anslutning till lagen inte följs.*

***4 kap. 4 §*** *Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsyn.*

***4 kap. 5 §*** *Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.*

***4 kap. 6 §*** *Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 4 och 5 §§. Ett sådant föreläggande får förenas med vite.*

***4 kap. 7 §*** *Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 4 och 5 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.*

***4 kap. 8 §*** *Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare. Regeringen får meddela föreskrifter om säkerhetsrevisioner.*

***4 kap. 9 §*** *Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av denna lag.*
*En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.*

**Kommentar**: Omfånget som beskrivs i de nya reglerna för cybersäkerhet kan svälla ytterligare då det ger tillsynsmyndigheterna möjlighet att precisera kraven ytterligare och inkluderar flera fall där det ger regeringen eller myndigheter möjlighet att införa sekundär lagstiftning med specificerade krav för följande:

- riskhanteringsåtgärder (kapitel 3, artikel 1)
- systematiskt och riskbaserat informationssäkerhetsarbete (3 kap. 2 §)
- utbildning om riskhanteringsåtgärder (kapitel 3, artikel 3)
- vad utgör en större incident (3 kap. 4 §)
- åtgärder för incidentrapportering (kapitel 3, artiklarna 8)
- säkerhetsrevisioner (4 kap. 9 §).

# En informationssäkerhetspolitik

Avslutningsvis vill TechSverige framföra att, utöver frågan om vikten av en marknadsledd utveckling inom informations- och cybersäkerhet och kompetensförsörjningsfrågan är förmodligen den statliga ansvarsfördelningen en av de viktigaste frågorna för höjd informations- och cybersäkerhet brett i samhället. Som noterats i inledningen, går den nog inte i praktiken att skilja ut från andra offentliga åtaganden och lagstiftning från EU. Ansvarsfördelningen är ett angeläget men också ett svårt arbete. Flera regeringar har nog också underskattat komplexiteten eller åtminstone inte handlat efter en bred och genomarbetad syn på området.

Vad gäller den statliga ansvarsfördelningen och t.ex. huvudmannaskap för informations- och cybersäkerhet krävs en mer genomgripande utredning än vad denna och tidigare regeringar har låtit göra.

Det krävs ett grundläggande arbete om det offentliga åtagandet, definitioner och avgränsningar (t.ex. informations- och cybersäkerhetsarbete jämfört med informationssäkerhetspolitik), nuvarande lagstiftning och ansvarsfördelning inom flera områden liksom en klarsyn om vilka mål som ska nås inom ramen för det offentliga åtagandet.

Kort sagt – det finns ett behov av en informationssäkerhetspolitik.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Fredrik Sand
näringspolitisk expert