Tullverket
Rättsavdelningen

YTTRANDE

Datum
2024-05-28

Dnr
STY 2024-181

Ert datum
2024-05-28

Er referens
Fö2024/00496

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Tullverkets ställningstagande

Tullverket har granskat delbetänkandet mot bakgrund av myndighetens uppdrag och hur förslaget kan komma att påverka myndighetens verksamhet. Tullverket delar inte utredningens uppfattning om att Tullverket inte bör undantas från den nya lagens tillämpningsområde.

Tullverket noterar att utredningen i sin analys endast tagit ställning till om cybersäkerhetslagen kommer att vara tillämplig för Tullverket utifrån myndighetens brottsbekämpande uppdrag.[1]

Tullverket anser till skillnad från utredningen, att myndigheten med stöd 1 kap. 11 § i förslaget på ny cybersäkerhetslag ska vara undantagna från lagens tillämpningsområde på den grunden att den övervägande delen av Tullverkets verksamhet är att betrakta som säkerhetskänslig.

Tullverket bedriver säkerhetskänslig verksamhet enligt 1 kap. 1-2 §§ i säkerhetsskyddslagen (SFS 2018:585). Med säkerhetskänslig verksamhet följer åtgärder och kontroller som grundar sig i Tullverkets säkerhetsskyddsanalys, se 2 kap. 1 § säkerhetsskyddslagen. Det är med utgångspunkt i säkerhetsskyddsanalysen som omfattningen av en myndighets säkerhetskänsliga verksamhet kan synliggöras. Däremot är analysen säkerhetsskyddsklassificerad i sig varför Tullverket är förhindrad att i detalj utveckla resonemanget i detta led. Det framgår dock av myndighetens säkerhetsskyddsanalys att Tullverket, till övervägande del, bedriver säkerhetskänslig verksamhet.

Flera segment i Tullverkets verksamhet utgörs av processer som till övervägande del är samhällsviktiga och säkerhetskänsliga samtidigt. Därmed är dessa delar av myndighetens verksamhet en del av totalförsvaret, vilket får genomslag såväl i säkerhetsskyddsanalysen som i Tullverkets kontinuitetsplan. Antagonistiska hot och potentiella skadekonsekvenser i

[1] Delbetänkandet, s. 163 f.

Tv 292.2 Utgåva 3 Januari 2024

förhållande till Tullverkets uppdrag som gränskontrollmyndighet skulle drabba samhället på nationell nivå.[2] Det sagda torde innebära att myndigheten som sådan bör inordnas under samma kategori säkerhets- och försvarsmyndigheter som de som i förslaget till cybersäkerhetsförordning[3] undantagits från cybersäkerhetslagens tillämpningsområde.

Mot den nu angivna bakgrunden avstyrker Tullverket utredningens förslag i nu aktuell del och anser att Tullverket bör undantas från cybersäkerhetslagens tillämpningsområde.

Övriga synpunkter

Oaktat Tullverkets inställning om att myndigheten inte ska omfattas av cybersäkerhetslagen vill Tullverket lämna följande synpunkter.

Undantag för offentliga verksamhetsutövare (avsnitt 5.5.4)

För myndigheter som bedriver både säkerhetskänslig verksamhet och brottsbekämpning kommer det att behöva göras en gränsdragning avseende vad i miljöerna som faller utanför vissa delar av cybersäkerhetslagens tillämpningsområde enligt 1 kap. 12 § i förslaget. Det kommer att bli en utmaning att hålla isär de olika delarna i de nätverk och informationssystem som i vissa delar - men inte alla - stödjer säkerhetskänslig verksamhet eller den brottsbekämpande verksamheten. I teorin skulle en sådan kartläggning gå att göra men i praktiken blir det svårt. När en incident påverkat säkerhetskänslig verksamhet och/eller den brottsbekämpande verksamhet kommer cybersäkerhetslagen till exempel inte att vara tillämplig på de delarna av hanteringen. Det som kvarstår av incidenthanteringen och som omfattas av lagen kommer då endast att utgöra en förhållandevis avgränsad del. Tullverket ställer sig frågande till vilken nytta den gränsdragningen gör för cybersäkerheten i stort när syftet med NIS2 varit att åstadkomma dels ett bättre helhetsskydd, dels en högre lägstanivå av cybersäkerhetsskydd hos samtliga aktörer som omfattas av lagen.

Riskhanteringsåtgärder och incidentrapportering (avsnitt 7)

Merparten av de åtgärder som presenteras i 3 kap. är i och för sig överlämnade till föreskriftsrätten hos respektive tillsynsmyndighet men det kan ändå konstateras att delbetänkandet ger förslag på aktiviteter som skulle innebära en ökad administrativ börda. Det riskerar dock att behöva ske på bekostnad av resurser som i dag används till att genomföra säkerhetsåtgärder. Många myndigheter arbetar redan i dag med etablerade processer och arbetsmetoder som överlappar de förslag som lämnas i delbetänkandet. Detta arbete sker dessutom till stora delar inom ramen för befintliga incident- och åtgärdsprocesser kopplat till bland andra Säkerhetspolisen, Integritetsskyddsmyndigheten och Myndigheten för samhällsskydd och beredskap. Incidentrapporteringen bör även harmoniseras med MSBFS 2020:8[4] gällande exempelvis tidsfrister för varning och

---

[2] Delbetänkandet s.158 och Prop. 2017/18:89 s.44 ff.

[3] Se 6 § förslag till förordning om cybersäkerhet (delbetänkandet s. 57 samt s. 157 ff.).

[4] Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter.

incidentanmälan. För myndigheter som bedriver såväl säkerhetskänslig som brottsbekämpande verksamhet, utöver verksamhet som inte kan kategoriseras som någondera av ovanstående, blir gränsdragningen än besvärligare.

Att applicera ytterligare riskhanteringsåtgärder och andra administrativa aktiviteter riskerar att underminera syftet med och tillämpningen av 3 kap. i förslaget och artikel 1 i NIS2. Det kan ifrågasättas om förslaget i praktiken kommer att innebära ökad cybersäkerhet, eller åtminstone i vilken utsträckning och på bekostnad av vad.

Tillsyn (avsnitt 8)

Tillsynsprocessen enligt förslaget till ny cybersäkerhetslag bygger på att tillsynsmyndigheten ska beredas tillgång till information och lokaler som behövs för att kunna genomföra tillsynen ifråga.[5] Tullverket vill understryka att de gränsdragningsproblem som uppstår för en myndighet som till del någon del bedriver säkerhetskänslig och/eller brottsbekämpande verksamhet inte ska underskattas. Det kan många gånger i princip vara omöjligt att skapa ett avgränsat segment i en verksamhet som inte är säkerhetskänslig till sin karaktär, i syfte att låta en annan tillsynsmyndighet än Säkerhetspolisen kunna granska den. Det finns risk att ett underlag för granskning i den situationen blir obegripligt.

Säkerhetsrevisioner och säkerhetsskanningar (avsnitt 8.4.6)

Angående frågan om säkerhetsrevisioner och säkerhetsskanning ser Tullverket vissa potentiella praktiska hinder. En myndighets säkerhetsfunktioner och säkerhetsåtgärder är i regel väl integrerade i myndighetens arkitektur och digitala infrastruktur. I de fall myndighetens it-miljö stödjer brottsbekämpande och säkerhetskänslig verksamhet måste säkerhetsrevisionerna avgränsas från dessa områden, vilket begränsar säkerhetsrevisionerna i en sådan omfattning att syftet riskerar att gå förlorat.

Säkerhetsskanningar eller sårbarhetsskanningar är en viktig funktion för att säkerställa att it-miljön inte är exponerad för kända sårbarheter men också en naturlig del av myndigheters interna granskning. Säkerhetsskanningar behöver dock genomföras på ett sådant sätt att resultatet ger en rättvis bild av myndighetens samlade cybersäkerhetshetsförmåga. Då it-stöd som stödjer brottsbekämpande respektive säkerhetskänsliga verksamheter är exkluderade från tillsynsområdet blir utförandet av säkerhetsskanningen problematisk och resultatet ger en allt för smal och fragmenterad bild av en myndighets cybersäkerhetsförmåga. Vidare är säkerhetsskanning ett komplext verktyg och skanning behöver därför ske kontinuerligt och omhändertas som en integrerad del i det dagliga säkerhetsarbetet.

---

[5] Delbetänkandet, s 205 ff.

Ärendets handläggning

I detta ärende har vikarierande generaltulldirektören Johan Norrman beslutat. Föredragande har varit verksjuristerna Åsa Kristensson och Johan Wirdenäs. I den slutliga handläggningen har även vikarierande överdirektören Bodil Taylor och tillförordnade rättschefen Cecilia Riddselius deltagit.

TULLVERKET

Johan Norrman

Kopia till:
Finansdepartementet, S3
Tullverket
Verksledningsstaben
Kommunikationsdelningen
Säkerhetsstaben och it-avdelningen