Rättsenheten
Robert Scherman
Verksjurist

Datum
2022-01-24

Diarienummer
2021-18090-4

Mottagare
Försvarsdepartementet

Er referens

Betänkandet Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Säkerhetspolisen välkomnar utredningens förslag i betänkandet och har följande synpunkter på detsamma.

12 Certifiering av nätverks- och informationssystem

Säkerhetspolisen delar utredningens bedömning att det i dagsläget inte finns skäl att införa något slags nationell certifieringsordning för IKT-produkter, -tjänster och -processer (hädanefter IKT-produkter) i nätverks- och informationssystem i säkerhetskänslig verksamhet. Detta av i huvudsak samma skäl som utredningen redogjort för.

Det är för tidigt att säga vilken påverkan som framtida certifieringar inom ramen för det europeiska ramverket för cybersäkerhetscertifiering kan få för möjligheten att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Utvecklingen och effekterna av det nya europeiska ramverket bör avvaktas och utvärderas innan en nationell särskilt anpassad ordning för certifiering av IKT-produkter i säkerhetskänslig verksamhet övervägs ytterligare. Skulle en sådan ordning därefter anses lämplig delar Säkerhetspolisen utredningens bedömning att tillsynsmyndigheterna själva kan föreskriva om det med stöd av 8 kap. 6–7 och 10 §§ säkerhetsskyddsförordningen.

Mot denna bakgrund – och då övriga relevanta delar av det föreslagna uppdraget till Försvarets materielverk kan anses i stora delar omhändertaget genom regeringsbeslutet den 10 december 2020 (Fö2019/01330) angående det nationella cybersäkerhetscentrets uppdrag och verksamhetsinriktning – menar Säkerhetspolisen att behovet av det föreslagna särskilda uppdraget till Försvarets materielverk kan ifrågasättas.

13 Krav på godkännande och utvidgat samrådsförfarande för informationssystem

Säkerhetspolisen instämmer i utredningens bedömningar och tillstyrker förslaget i stort. Säkerhetspolisen önskar dock göra följande medskick.

Säkerhetspolisens uppfattning är att den föreslagna lydelsen av 3 kap. 1 § säkerhetsskyddsförordningen bör omformuleras. Detta eftersom begreppet tillsynsområde i förhållande till Säkerhetspolisen och Försvarsmakten, så som detta begrepp definieras i 8 kap. 1 § säkerhetsskyddsförordningen (2021:955), inte tydligt omfattar verksamhetsutövare som hör till annan tillsynsmyndighets tillsynsområde.

Såvitt avser lydelsen av föreslagna 3 a kap. 1 § andra stycket säkerhetsskyddslagen, menar Säkerhetspolisen att den sista meningen bör lyda: ”Verksamhetsutövaren ska också *i vissa fall* samråda enligt 2 §.” Detta eftersom samrådsskyldigheten endast aktualiseras i vissa fall.

Såvitt avser lydelsen av föreslagna 3 a kap. 4 § säkerhetsskyddslagen, menar Säkerhetspolisen att bestämmelsen bör lyda som följer.

> Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift*, eller i väsentliga avseenden förändras,* förrän *förfarandet* har godkänts från säkerhetssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.

Därutöver önskar Säkerhetspolisen påtala att det kan framstå som förvirrande att begreppet samrådsmyndighet återinförs (jfr föreslagna lydelser av 3 a kap. 2, 3 och 5 §§ samt 7 kap. 2 a och 9 §§ säkerhetsskyddslagen jämte 3 kap. 1 § säkerhetsskyddsförordningen). Detta eftersom samma begrepp med annorlunda betydelse utmönstrades ur säkerhetsskyddslagen per den 1 december 2021.

14 Tillgång till informationssystem vid tillsyn

Säkerhetspolisen instämmer i utredningens bedömningar och tillstyrker förslaget i stort. Säkerhetspolisen önskar dock göra följande medskick.

I likhet med utredningens bedömning menar Säkerhetspolisen att behovet av att kunna genomföra tekniska säkerhetsgranskningar inom ramen för tillsyn under säkerhetsskyddslagen är akut, och att en rätt för ansvarig tillsynsmyndighet att kunna förelägga verksamhetsutövare att ge myndigheten tillgång till nätverks- och informationssystem är nödvändig. Av utredningen framgår dock inte tydligt skälen till detta. Säkerhetspolisen har i skrivelse till utredningen den 4 maj 2021 utvecklat skälen enligt följande.

> Granskning av informationssäkerheten i ett informationssystem behöver ske genom aktiv kontroll i systemet tillsammans med dess omkringliggande infrastruktur, s.k. penetrationstestning. I de flesta

> fall är det således inte tillräckligt att besiktiga systemet okulärt och passivt. Den ökade digitaliseringen även av säkerhetskänslig verksamhet innebär att behovet av att kontrollera skyddsåtgärder i informationssystem genom penetrationstestning ökar. För att kunna genomföra fullgod tillsyn av säkerhetsskyddsåtgärder i informationssystem behöver Säkerhetspolisen således, utöver rätten att få tilltillträde till lokaler och utrymmen, ha rätt att få tillträde till själva informationssystemet i syfte att kunna genomföra penetrationstester. En sådan rätt omfattas inte av det nu liggande förslaget till ändringar i säkerhetsskyddslagen [prop. 2020/21:194], vilket betyder att Säkerhetspolisen inte inom ramen för sin tillsyn kommer att kunna granska informationssystem i säkerhetskänslig verksamhet i den utsträckning som behövs. Det är därför mycket angeläget att frågan om Säkerhetspolisens rätt att få tillträde även till informationssystem regleras i säkerhetsskyddslagen.

Säkerhetspolisen noterar att den föreslagna lydelsen av tillägget i 6 kap. 3 § säkerhetsskyddslagen, om att tillsynsmyndigheterna i vissa fall ska ha rätt att få tillgång till informationssystem, kan upplevas som missvisande. Det kan finnas behov av att i lagen tydliggöra att syftet med denna tillgång är att tillsynsmyndigheten ska kunna göra tekniska säkerhetsgranskningar.

Utom såvitt avser ett fåtal tillsynsmyndigheter ser Säkerhetspolisen stora svårigheter med att tillsynsmyndigheterna ska kunna upprätta och vidmakthålla en förmåga att själva genomföra tekniska säkerhetsgranskningar. I syfte att i vart fall delvis komma till rätta med denna problematik menar Säkerhetspolisen att regeringen bör överväga att tydliggöra att den omständigheten att det finns behov av en teknisk säkerhetsgranskning hos en viss verksamhetsutövare kan utgöra *särskilda skäl* för Säkerhetspolisen och Försvarsmakten att, inom sina respektive tillsynsområden, ta över denna del av tillsynsansvaret för en verksamhetsutövare enligt 8 kap. 3 § säkerhetsskyddsförordningen. I anslutning härtill bör regeringen överväga att ändra lydelsen i 8 kap. 3 § säkerhetsskyddsförordningen så att det uttryckligen framgår att tillsynen kan övertas helt eller *i del*. På så vis skulle Säkerhetspolisen respektive Försvarsmakten vid behov kunna ta över endast den del av tillsynen som avser teknisk säkerhetsgranskning av nätverks- och informationssystem, medan tillsynsansvaret i övrigt ligger kvar hos tillsynsmyndigheten.

Därutöver bör regeringen överväga att ge Säkerhetspolisen och Försvarsmakten i egenskap av samordningsmyndigheter i uppdrag att tillhandahålla tillsynsmyndigheterna inom sina respektive tillsynsområden förmåga (personell såväl som teknisk) att genomföra tekniska säkerhetsgranskningar. Tillsynsmyndigheterna bör i sådant fall ha rätt att besluta om en tillsynsåtgärd där en sådan resurs behövs endast efter samråd med Säkerhetspolisen eller Försvarsmakten. Detta i syfte att motverka att Säkerhetspolisens eller Försvarsmaktens resurser tas i anspråk för tillsynsåtgärder av i sammanhanget mindre vikt.

9.5 Konsekvensbeskrivning

Utredningens förslag om tillsynsmyndigheternas tillgång till informationssystem för att kunna utföra tekniska säkerhetsgranskningar innebär en tydlig ambitionshöjning i tillsynsarbetet. Även om Säkerhetspolisen redan nu har vissa resurser att genomföra tekniska säkerhetsgranskningar inom ramen för sin rådgivning innebär denna ambitionshöjning att nya metoder måste tas fram och utvecklas över tid. Detta kommer att kräva att ytterligare resurser tillförs Säkerhetspolisen.

Ytterligare resurser krävs även i det fall Säkerhetspolisen får i uppdrag att tillhandahålla personella och tekniska förmågor inom ramen för andra tillsynsmyndigheters granskningar, och/eller väljer att utveckla en praxis där Säkerhetspolisen, när behov för teknisk granskning finns, övertar tillsynen av en enskild verksamhetsutövare från en annan tillsynsmyndighet.

Det framstår som sannolikt att såväl behovet som antalet och omfattningen av tekniska säkerhetsgranskningar kommer att vara föremål för en exponentiell ökning över tid.

Säkerhetspolisens behöver sammanfattningsvis på sikt tillföras ytterligare medel om uppskattningsvis minst tio miljoner kronor årligen. Säkerhetspolisens anslag kan förslagsvis ökas med fem miljoner första året och sedan ytterligare fem miljoner andra året. Detta mot bakgrund av att uppbyggandet av förmågan kommer att tas i olika steg.