Säkerhetspolisen

REMISSVAR

Datum: 2024-05-27
Diarienummer: 2024-6497-2

Mottagare:
Finansdepartementet
103 33 Stockholm
Referens:

En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur

Säkerhetspolisen tillstyrker förslaget i den remitterade promemorian och lämnar följande synpunkter.

Krisledning och krishantering på cybersäkerhetsområdet hos identifierat samhällsviktig eller säkerhetskänslig verksamhet är i behov av bättre samordning. Det föreligger alltjämt oklarheter i hur den närmare ansvars- och rollfördelningen ska se ut mellan nu aktuell funktion, kommande cyberkrishanteringsmyndighet (jfr SOU 2024:18), Nationellt cybersäkerhetscenter (NCSC) respektive CSIRT-SE/CERT-SE. Det bör utredas vidare vad de olika aktörernas krishanteringsförmågor och -uppdrag ska bestå i, hur krishanteringen bäst struktureras, inklusive hur ansvar och roller myndigheter emellan fördelas, samt i vilken utsträckning även andra sektorer än den finansiella sektorn är i behov av egen, sektorsspecifik krishanteringsförmåga.

Angående samverkan mellan den nya föreslagna funktionen och NCSC (s. 91 i PM) menar Säkerhetspolisen att det föreslagna informationsutbytet inte bör, så som det står skrivet, vara begränsat till antagonistiska cyberattacker, utan även omfatta andra betydande IT-incidenter.

Säkerhetspolisen har även följande mindre, närmast redaktionella synpunkter.

Vad som menas med begreppet säkerhetskänslig verksamhet (s. 20 i PM) bör justeras till följande: ”Med säkerhetskänslig verksamhet menas sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.” Säkerhetspolisen noterar vidare att begreppen cyberattack och cyberangrepp, enligt den angivna definitionen (samma sida), inte omfattar attacker som härstammar från brister i den fysiska säkerheten eller personalsäkerheten, t.ex. att någon förmås eller luras att stoppa in ett infekterat USB-minne i en enhet. Möjligen kan med anledning därav även begreppen it-attack och it-angrepp vara värda att nämna i sammanhanget, eftersom de inte är begränsade i förhållande till på vilket sätt attacken sker. Därtill skulle det kunna förtydligas att begreppet cyberrymden (samma sida) omfattar såväl all kommunikation via internet som telekommunikation.

Definitionen av säkerhetsskydd (s. 31 i PM) lyder lämpligen: ”Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.”

Beskrivningen av kravet på anmälan av säkerhetshotande händelse kopplas endast till informationssäkerhet (s. 32 i PM). Det är i sammanhanget relevant att sådan anmälan ska göras även i händelse av incident med koppling till personalsäkerhet eller fysisk säkerhet.

Detta remissvar har beslutats av chefsjuristen Per Lagerud efter föredragning av verksjuristen Robert Tolonen Scherman