2021-12-16

Dnr RG 2021/817

Försvarsdepartementet
Jakobsgatan 9, 11152 Stockholm
fo.remissvar@regeringskansliet.se

Remissvar över betänkandet SOU 2021:63

Sveriges säkerhet – behov av starkare skydd för nätverks-och-informationssystem (Fö2021/00796)

Sammanfattning

Riksgäldskontoret (Riksgälden) ställer sig positiv till utredningens förslag och slutsatser. Riksgälden ställer sig särskild positiv till att det föreslås utökade möjligheter till samråd med samrådsmyndigheter (Säkerhetspolisen eller Försvarsmakten). Riksgälden ser att samråden och möjligheten att kunna ta del av deras expertis tillsammans med utbildning av IT personal är centralt för att uppnå starkare skydd för nätverks- och informationssystemen.

Utöver dessa kommentarer lämnar Riksgälden även följande synpunkter:

- Krav på certifierade IKT-produkter i säkerhetskänslig verksamhet ger inte alltid tillräckligt skydd av flera skäl:

- *”Hotaktörer ligger alltid steget före”* då certifierade IKT-produkter ofta inte är de senaste på marknaden samt att certifieringar av liknande slag (Common Criteria/CC) historiskt har baserats på en specifik och fastställd konfiguration för respektive produkt. Hotaktörer har inte dessa begränsningar och har därför ett försprång på området.

- Certifierade IKT produkter kan komma att ingjuta en känsla av falsk säkerhet om de blir obligatoriska komponenter i myndigheters IT-miljöer. En annan strategi skulle kunna vara att förbjuda produkter/komponenter/leverantörer som bedömts vara osäkra t.ex. genom avsnitt 5 Strategisk prioritering och 5.1.2 Vidareutveckla analysförmåga av hårdvara i ”Samlad informations och cybersäkerhetshandlingsplan 2019-2022 : redovisning 2021”.

- Det är i tillverkarens intresse att genomföra certifiering av produkter, detta ger ett gap mellan produkter som används av myndigheter och produkter där tillverkaren är intresserad av att genomföra en certifiering.

Riksgäldskontoret
ORG.NR. 202100-2635
POSTADRESS POSTAL ADDRESS SE-103 74 Stockholm Sweden
BESÖK VISITORS Olof Palmes gata 17
TELEFON TELEPHONE NAT. 08 613 45 00 INT. +46 8 613 45 00
TELEFAX NAT. 08 21 21 63 INT. +46 8 21 21 63
INTERNET riksgalden@riksgalden.se www.riksgalden.se

- Det bör läggas stor vikt på kontinuerlig utbildning och eventuell certifiering av personal för att delvis hantera och motverka risker som föreligger kring IKT-produkter.

Utbildning och eventuell certifiering av personal skulle med fördel kunna delas upp i olika utbildningar och certifieringar där vissa rör t.ex. operativ IT-säkerhet, IT-resiliens, säker programmering/kodning, ”Threat hunting”. Det öppnar för nya karriärvägar för befintlig personal. Att utbilda personal harmonierar också väl med de ambitioner som de myndigheter som idag ingår i det nationella cybersäkerhetscentret (CFCS) redogjort för i ”Samlad informations- och cybersäkerhetshandlingsplan 2019-2022 : redovisning 2021”.

CFCS skulle kunna utbilda och certifiera IT personal hos myndigheter i säker arkitektur och design av IT-system.

Riksgälden ser också att de strategiska prioriteringarna som redovisas i ”Samlad informations- och cybersäkerhetshandlingsplan 2019-2022 : redovisning 2021” innehåller konkreta förmågehöjande åtgärder som om de införs och systematiseras, tillsammans kommer att nå en avsevärd effekt- och förmågehöjning hos civila aktörer vilket också leder till ett starkare skydd för nätverks- och informationssystem på ett mer holistiskt sätt.

- Följande samverkansområden och funktioner bör prioriteras:

- Främja kompetensutveckling genom att skapa en "resurspool" mellan olika myndigheter.
- CFCS driver samverkansprojekt för framtagande av normativa mallar för nätverks- och systemarkitektur.
- CFCS driver samverkansprojekt för framtagande av normativa mallar för härdning av system inklusive utbyte av erfarenheter, vad fungerar, vad fungerar inte.
- CFCS driver samverkan kring mallar för inställningar av loggning / spårbarhet i operativsystem och standard-produkter.
- CFCS driver framtagande av plattform för utbyte av realtids-information om aktuella hot, hotaktörer, tekniska indikatorer samt kritiska sårbarheter.
- CFCS ska kunna pröva förmåga hos myndigheter i t.ex. red- / blue-team övningar.
- CFCS driver skapande av "Övningsbank", både hotaktör- och haveriscenarion.
- CFCS ska kunna genomföra periodiska sårbarhetsanalyser på publikt exponerade tjänster över internet hos myndigheter.

I detta ärende har riksgäldsdirektören Hans Lindblad beslutat efter föredragning av Sergio Rojas. I den slutliga beredningen har även avdelningschefen Ingela Rindå, enhetscheferna Karin Olausson och Anders Brouzell, nätverkstekniker Lotta Hansell, Pawel Worach samt säkerhetsanalytikerna Gunnar Maxen och Tommy Gurell vid Säkerhetsenheten deltagit.

_____

Hans Lindblad, beslutande

_____

Sergio Rojas, föredragande