Remissvar
Hanteringsklass: Öppen R1 T1
Diarienummer RG 2026/270
2026-02-27

Myndigheten för civilt försvar
651 81 Karlstad
Ärendenummer 2025-03955

Remissvar från Riksgäldskontoret på policyer för ett starkare cybersäkerhetsarbete

(MSB 2025/03955)

Riksgäldskontoret (Riksgälden) vill med detta underlag lämna synpunkter på Myndigheten för civilt försvars (MCF) förslag till policyer för ett starkare cybersäkerhetsarbete

Definitioner och harmoniserade regelverk

Riksgälden förordar att man ser över definitioner och begrepp inom IT-området i policyn så att de är likalydande med EU-regelverkens definitioner på svenska och, om sådana saknas, internationellt allmänt tillgängliga förteckningar. Översättningar och specifikt svenska definitioner och begrepp föreslås föras in i termbanken.[1]

Vidare är det bra om kravställning och assuranskrav harmoniseras till struktur och innehåll med EU:s regelverk och standarder så som EECC, EUCC, CSA, CRA med flera. Därutöver rekommenderas att principerna om ömsesidigt erkännande tillämpas för andra länders nationella standarder, bland annat för molntjänster så som Tysklands C4 och C5 samt Frankrikes SecNumCloud.[2]

[1] https://www.iso.org/obp/ui och https://termbank-informationssakerhet.msb.se/
[2] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html, , https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html, https://cyber.gouv.fr/enjeux-technologiques/cloud/

Öppna standarder

Då det för närvarande refereras till standarder som kräver att användaren betalar bör det prövas om det är möjligt att tillämpa öppet tillgängliga standarder som är tillgängliga utan kostnad enligt 10 kap 7 § LOU.[3]

Stärkt säkerhet i digitala leveranskedjor

Digital suveränitet och brutna monoberoenden

Riksgälden vill lyfta vikten av att se över cybersäkerhetsbehoven över hela hotskalan samt vilka förmågor som behövs vid fredstida kris, höjd beredskap och krig.

Åtgärder som kommer att vidtas av det nationella cybersäkerhetscentret och dess partners

Vad gäller insamlingen genom Leverantörskedjekollen förordar Riksgälden att pröva om detta kan ske genom etablerade system för upphandlingsstatistik och ekonomisk redovisning, såsom Hermes och Kommun-Bas. Dessa redovisningssystem skulle kunna tillgodose behovet.

Åtgärder som regeringen rekommenderas att vidta

Riksgälden avstyrker *punkt 1* och förordar att ordinarie kanaler för inköpsstatistik kompletteras och nyttjas för strategisk leverantörsdialog i samverkan mellan NCSC, MCF, FM, FMV/CSEC, Adda och Statens inköpscentral för att tillgodose behovet i hela hotskalan.

Riksgälden avstyrker *punkt 2* gällande automatiserad insamling av de aggregerade informationsmängderna, härledingsbara till enskilda verksamhetsutövare. En sådan uppgiftsinsamling kommer troligtvis att omfattas av säkerhetsskydd.

Riksgälden tillstyrker *punkt 3* gällande digital suveränitet, med tillägg för diversifierade åtgärder för att stärka förmåga i hela hotskalan.

Åtgärder som verksamhetsutövare rekommenderas att vidta

Riksgälden tillstyrker *punkt 2* med tillägg för att Cybersäkerhetskollen behöver omformuleras till en traditionell revisionsrapport strukturerad efter ett etablerat ramverk inom cybersäkerhet, exempelvis EECC, NIST SP 800 53 eller ISO

[3] Konkurrensverkets ställningstagande 232/2024

27002:2022, samt att det tillhandahålls i ett redigerbart rådataformat och framledes automatiseras till maskinläsbara format.[4]

Riksgälden vill framhålla att de aggregerade resultaten i Cybersäkerhetskollen idag är svåra att härleda till enskilda kontroller i Cybersäkerhetskollen. Metodiken i NIST CSF 2.0 förordas då inriktningen för varje kontroll kan jämföras mot aktuell forskning kring åtgärders effektivitet i ett helhetsperspektiv, exempelvis från FOI eller ENISA Threat Landscape. [5]

Cybersäker upphandling

Riksgälden är positiv till initiativet. Som nämnts ovan bedömer Riksgälden att de nationella inköpscentralerna har en viktig roll i förbättrad kravställning då en stor del av inköpen sker genom deras ramavtal. Riksgälden skulle också se det positivt att få avropa från FMV:s ramavtal inom ramen för det civila försvarets behov.

I nuläget är de nationella ramavtalen individuellt utformade, både vad avser allmänna villkor och säkerhetskrav. Säkerhetskraven är något begränsade, fördelade över flera bilagor och ger omfattande preciseringsmöjligheter vid förnyad konkurrensutsättning. Det gör att det många gånger saknas förutsättningar för att tillämpa dem enligt principen alla villkor fastställda och avropsberättigade myndigheter riskerar att skapa ramavtal i ramavtalen.

Åtgärder för att uppnå målbilden

Vad gäller *punkt 3* förordar Riksgälden att de nationella inköpscentralerna genomför kontroller eller kontroller av leverantörernas egna tredjepartsrevisioner. Det innebär en säkerhetsrisk om kunskap om leverantörers säkerhetsåtgärder exempelvis skyddsåtgärder i datacenters sprids brett och det bör därför samordnas nationellt.[6]

Vidare rekommenderas att undvika nationella säkerhetskravkataloger utifrån det som redan är kravställt i andra länder eller internationella organisationer såsom OWASP, MITRE eller Common Criteria. Global harmonisering och standardisering är viktig. Riksgälden ser ett behov av metodstöd för att lära sig använda de befintliga standarderna och förstå hur de ska implementeras i

[4] https://pages.nist.gov/OSCAL/
[5] Identify, Protect, Detect, Respond, Recover samt FOI Försvarbarhet I cyberdomänen En litteraturstudie, FOI-R--5850—SE, 2025
[6] https://www.adda.se/upphandling-och-ramavtal/ramavtal-och-kategorier/avtalsuppfoljning/ från Adda respektive Statens inköpscentral https://www.avropa.se/ramavtal/uppfoljningsgruppen/

enskilda verksamhetsutövares kontext utifrån upphandlingsföremålens karaktär.

I detta ärende har chefen avdelning Stab Jörgen Eklund beslutat efter föredragning av säkerhets- och säkerhetsskyddschef Mikael Holmer.

RIKSGÄLDSKONTORET

Jörgen Eklund, beslutande

Mikael Holmer, föredragande