Ålands landskapsregering

PROTOKOLL

Nummer	Sammanträdesdatum
8	**26.10.2023**

Protokoll fört vid enskild föredragning

Regeringskansliet
Allmänna byrån, Digitaliseringsenheten, Rk1e

Beslutande	Föredragande	Justerat
Minister	IT-chef	
Fredrik Karlström	Jani Sjölund	

....

Nr 11
Tillsättande av programstyrgrupp för informationssäkerhetsprogrammet
ÅLR 2023/8411
6 Rk1e

Beslut

Landskapsregeringen ser att behovet av en säker och effektiv informationshantering ökar då kommande EU-lagstiftning (NIS2) ställer nya hårdare krav på informationshanteringen inom hela offentliga sektorn. Det ökade utbytet av digital information inom åländsk offentlig förvaltning och med nationella samt EU-system ökar dock samtidigt exponeringen för it-intrång, phishing, överbelastningsattacker, trojaner och ransomware.

Landskapsregeringen beslutade därför att tillsätta en programstyrgrupp med uppdrag att säkerställa att det offentliga Åland ska kunna ansluta sig till gemensamma nationella system och uppfylla kraven för NIS2-direktivet genom informationssäkerhetsprogrammet och dess tre delprojekt informationssäkerhet, hosting och tjänstefiering.

Informationssäkerhetsprogrammet ska uppfylla villkoren i relevanta ramverk och på så sätt möta de informationssäkerhetskrav som kommer att ställas vid fullvärdiga integrationer till nationella system och EU-system. En närmare beskrivning av uppdraget finns i bilaga 1.

Landskapsregeringen beslutade att utse

- Jani Sjölund, IT-chef och ordförande för programstyrgruppen, Landskapsregeringen
- Fredrik Karlström, Minister, Landskapsregeringen
- Runa Tufvesson, Byråchef och ägarrepresentant, Landskapsregeringen
- Christian Jansson, VD, Åda
- Andreas Perjus, Styrelseordförande, Åda
- Rickard Boije, Styrelseledamot, Åda

Som sekreterare och föredragande av mötesagendan fungerar av landskapsregeringen utsedd program- och projektledare.

Kommittéarvoden utbetalas enligt gällande regelverk och belastar moment 21200.

Arbetsgruppen ska slutföra sitt uppdrag senast den 31 december 2023.

Nr 12
Inköp av SOC 24/7-tjänst för att övervaka, analysera och hantera säkerhetsincidenter och hot mot IT-infrastrukturen
ÅLR 2023/8412

Beslut

Beslöt att köpa in SOC 24/7tjänst för att övervaka, analysera och hantera säkerhetsincidenter och hot mot landskapsregeringens IT-infrastruktur, från Dell Ab. Den årliga kostnaden om totalt 50 000 euro belastar budgetmoment 21200. Inköpet görs tillsammans med Åda Ab.

Motivering

Den allmänna utvecklingen inom säkerhetsområdet har föranlett behovet av att förbättra Landskapsregeringens IT-infrastruktur. Cyberhoten ökar i både komplexitet och allvarlighetsgrad och omfattar känslig information som personuppgifter och regeringsbeslut.

En SOC 24/7-tjänst är en förkortning av "Security Operations Center 24/7-tjänst". Det är en centraliserad enhet inom en organisation eller en tredjepartsleverantör som är specialiserad på att övervaka, analysera och hantera säkerhetsincidenter och hot mot IT-infrastrukturen dygnet runt, sju dagar i veckan (24 timmar om dygnet, 7 dagar i veckan).

Syftet med en SOC-tjänst är att förbättra och säkerställa informationssäkerheten genom att snabbt upptäcka och hantera säkerhetsincidenter, inklusive cyberattacker och hot, för att minimera deras påverkan på organisationen. Att investera i en SOC-tjänst är nödvändigt för att säkerställa att denna information förblir skyddad och inte hamnar i fel händer. Genom att införa en SOC 24/7-tjänst kan landskapsregeringen stärka sitt försvar genom att ha specialiserade experter som övervakar och hanterar hot i realtid.

Nr 13
Förnyelse av programvara
ÅLR 2023/8413

Beslut

Beslöts förnya programvara för säkerhetsövervakning och -analys enligt tidigare beslut 2022/8541. Den årliga kostnaden om 33 665 euro belastar budgetmoment 21200.

Motivering

Dagens säkerhetshot och -risker blir alltmer komplexa, IT-miljön är utsatt för hot dygnet runt samtliga dagar under året. Expertkunskap samt en proaktiv verksamhet i form av säkerhetsövervakning samt analys av incidenter är nödvändig.

Informationssäkerhetsprogrammet

Projektdirektiv

Godkännande av programmets direktiv och bilagor

Beställare/Programägare:	Programledare:
Jani Sjölund	Åsa Schmiedhofer Svender

1 Programmets namn/ identitet

Informationssäkerhetsprogrammet

2 Bakgrund

Ökad digitalisering i en orolig värld innebär ökad exponering för cyberhot mot hela offentliga Åland och det åländska samhället. Behovet av en ökad *nivå på informationssäkerhet* förtydligas från kommande EU-lagstiftning, NIS2*,* som börjar gälla från och med den 18 oktober 2024. Denna lagstiftning ställer tydliga krav på offentliga Åland och definierade medaktörer. Lagstiftningen *föreskriver även nivån för medaktörer av kritisk infrastruktur och samhällsviktiga tjänster.*

- Informationssäkerhet förutsätter rätt teknik, ett systematiskt arbete och specialistkompetens inom flera sakområden. Med tanke på kostnader, tid för verksamhetsutveckling och begränsadtillgång till nödvändig kompetens bör stöd för informationssäkerheten erbjudas med likvärdiga tjänster till Ådas alla kunder.
- För att kunna erbjuda hela offentliga Åland informationssystem som uppfyller kraven från NIS2 och möjliga certifieringar ska programmet utveckla tekniska förutsättningar för likvärdiga it-tjänster med bland annat en skalbar hostingmiljö som uppfyller NIS2-standarder.
- *Programmet ska också utveckla kompetens, processer och-skalbara tjänster och arbetssätt som kan erbjudas till alla Ådas ägare. Dessa tjänster ska ge ägarna likvärdiga och kostnadseffektiva då flera kunder kan dela på samma resurser.*
- *Kostnadseffektiv, skalbar informationssäkerhet byggs-genom tre projekt*
  - *Hosting*
  - Informationssäkerhet
  - Erbjudandet av it som tjänst till Ådas kunder

3 Effektmål

*Syftet är också att **Åda ska kunna erbjuda sina ägare tjänster som blir kostnadseffektiva och skalbara**. Dessa tjänster följer kvalitetsramar så att dessa uppfyller de säkerhetskrav som ställs för integration med lokala, nationella och EU-system*

4 Kontaktpersoner

- *Näringsminister, Fredrik Karlström*
- *LR IT- förvaltning och projektets beställare, Jani Sjölund*
- *LR ägarstyrning, Runa Tufvesson*
- *Åda styrelseordförande, Andreas Parjus*
- *Åda VD, Christan Jansson*
- *Åda styrelse, Richard Boije*
- *Specialist informationssäkerhet, Virginia Horniak*

5 Tidsplan och kalkyl för förberedelserna

Åtagande t o m	Tidpunkt	Kalkyl timmar	Kalkyl utlägg
BP2	2023-09-28	80 h	
BP3	2023-10-12	80 h	
Projektanalys	2023-11-06	60 h	

6 Programmets mål, krav och önskemål

Programmets mål är att Åda har skalbar teknik, processer och kompetens för att utveckla och vidmakthålla skalbara och kostnadseffektiva it-tjänster med informationssäkerhetsnivå enligt NIS2. Dessa tjänster kommer att erbjudas genom en certifierad hostingtjänst. Framtagning av resultatet kommer att utföras i tre projekt:

- Hosting
- Informationssäkerhet
- Erbjudandet av it som tjänst till kunderna

6.1 Projekt- Hosting

Målet med detta projekt är att utveckla en teknisk plattform för hosting som är redo att ta in LR Allmänna förvaltningen, utvalda resurser enligt separat migrationsprojekt, från och med november 2024 Redo att starta implementationsprojekt för övriga kunder fr o m och april 2025.

- *Etablerad hostingmiljö*
- *Lokal molntjänst- ÅLCloud*
- *Datalager- Åland*
- *Redundans-Dubbla hallar*
- *Intern realisering och processer dokumenterade*
- *Förvaltningsplan för framtida drift av teknik, arbetssätt och kompetens*
- *NIS2 följsamhet*
- *Katakri 3 nivå, proaktiv processmognad*
- Underlag till projektet ”Erbjudandet av it-som-tjänst till kunderna” då programmet utvecklar denna tekniska plattform till ett tydligt kunderbjudande ”hosting som tjänst” med ny affärsmodell, priser, avtalsvillkor m.m.

6.2 Projekt- Informationssäkerhet

Detta projekt fokuserar på processer, kunskap och systematiken enligt NIS 2 minimikraven samt ramverket Katakri 3.
Omfattningen är Ådas verksamhet, erbjudanden för it-som-tjänst samt av Åda ägda resurser- exempel lokaler, serverhallar, infrastruktur, data, applikationer, processer, kompetenser leverantörsrelationer.

Programmet ska leverera:

- Följsamhet med NIS2
- Följsamhet enligt Katakri 3 enligt externa återkommande revisioner
- Etablerat ramverk teknik, kompetenser, processer, roller, rutiner för informationssäkerhet hos Åda
- Förändring av processer och kompetenser från NIS-> NIS2
- SOC, Security Operations Center-Strukturerat arbetssätt och organisation för informationssäkerhetens ledningscentral på Åda
- *Förvaltningsplan förvaltar och vidmakthålla följsamhet NIS2, Katakri nivå 3 med extern revision vartannat år*
- *GAP analys- Nuläget- GAP – Åda*
- *Underlag till projektet Erbjudandet av it-som-tjänst till kunderna*

Programmet ska också leverera metod och kunskapsöverföring till LR allmänna förvaltningen som kan innehålla:

- Workshopledning, 2 tillfällen med LR allmänna förvaltningen- GAP analys och självdiagnos- LR allmänna förvaltningens säkerhetsgrupp
- Utbildning LR allmänna förvaltningen- Initial utbildning 3 tillfällen
- Analys- Rekommendation för uppdateringar av LR molnpolicy

6.3 Projekt- Erbjudandet av it-som-tjänst till kunderna

Målet med detta projekt är att erbjuda tjänster som är kostnadseffektiva, skalbara och uppfyller NIS2-kraven. Detta inkluderar:

- *Erbjudandet till kunden- Tjänstebeskrivning, Avtal, Affärsmodell, Pris,*
- *Stödjande material för kundens implementationsprojekt och mottagning i sin verksamhets förvaltning - Kundens check-lista samt grundförutsättningar för gemensam informationssäkerhet*
- *Förvaltningen på Åda- Ådas styrning av effektiv och skalbar tjänsteleverans*
    - *Intern realisering och processer-Teknisk lösning, de fem processerna, KPI-mål*
    - *NIS2, Katakri nivå 3 följsamhet*
    - *Pris och Kalkylunderlag*
    - *Etablerad förvaltning med förvaltningsplaner och målrapportering av processen*

NYA tjänster:

- Hosting som tjänst,
- Arbetsplats som tjänst
- Informationssäkerhet- Kompetensstöd
- Kompetensstöd för SOC till kunder
- AD och lösenordshantering- självservice

Anvisningar samt grundförutsättningar för medaktörernas informationssäkerhet
Förtydliga och addera grundförutsättningar för medaktörers:

- AD och lösenordshantering
- Infrastruktur
- Cybersäkerhet

6.4 Projekt-Informationssäkerhet, fördjupning

Säkerhetsåtgärder – minimikrav för att Ådas verksamhet och dess kvalitetssäkrade tjänster ska möta NIS2 till 1 oktober 2024. *2024 - Art. 21.2 NIS-2* *https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2555&qid=1685001673634#d1e3267-80-1*
Åtgärderna ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter
Åtgärderna ska vara etablerade på Åda med dedikerade roller, process, rutin och målrapportering till LR för det löpande arbetet efter projektets slut

Minst inbegripa följande minimikrav **enl. tolkning från Tech-Law**

a) Strategier för riskanalys och informationssystemens säkerhetsnivå
b) incidenthantering
c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, krishantering
d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer
e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inbegripet hantering av sårbarheter och sårbarhetsinformation
f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet
g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet
h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering
i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning
j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem

Underlag till Erbjudandet

- Informationssäkerhet- kompetensstöd- utbildning LR allmänna förvaltningen- x antal tillfällen
- SOC som instruktionsbaserad tjänst
- Utbildning- utbildningsmaterial för grundläggande kompetensutveckling
- Stödjande material för att identifiera behov av återkommande regelbunden kompetensutveckling för kunder
- GAP analyser- Stöd för kundens självdiagnos med analys av eget nuläge, GAP till NIS2
- Kundens check-lista för HUR respektive ägare kvalificerar sin verksamhet för att delta i gemensamma IT-system med kontrollerad nivå på sin del av informationssäkerheten.

***Verksamhetsutveckling på Åda med arbetssätt från NIS*-> NIS2**

- Befintliga processer ex Major Incident samt SÄPO tjänsten
- Medaktörer och underleverantörer
- Upphandling
- Avtal

Åda SOC- Security Operational Centre
Etablerad funktion och process med dedikerad drift och förvaltningsledning för att leda och integrera Ådas informationssäkerhet med Ådas övriga funktioner och processer. KPI-mål och rapportering

7 Avgränsningar

- Förstudie, Implementation och driftsättning för kunden ingår inte i programmet utan offereras separat.
- Följsamhet med NIS2 och Katakri för kundägda- processer, kompetens, teknik, resurser, inkluderar även data och information, ingår inte i projektmålen
- Omfattningen av tester beror på LR allmänna förvaltningens deltagande samt vilken strategi som avtalas för piloten och migrering till Hosting som tjänst.

8 Tidpunkt

Programmet genomföres från 2023- 2025

- Inkrementella leveranser sker fortlöpande under 2023-2025
- Tidig deadline för informationssäkerheten
    - NIS2 följsamhet för Åda oktober 2024

9 Kostnad

Totalt 1 000 000 Euro fördelas enligt följande uppskattning

Programledning och projekten	**2023**	**2024**	**2025**
Hosting	120’	180’	100’
Informationssäkerhet	20’	200’	100’
Erbjudandet av IT som tjänst till kunderna	60’	120’	100’
Totalt	**200’**	**500’**	**300’**

10 Programmets prioritering av målbilden

Önskemål för prioritering av projektets målbild.

Prioritering: 0.4 Resultat 0,4 Tidpunkt 0,2 Kostnad

11 Finansiering

Programmet finansieras genom reserveringar i tilläggsbudget 1/2023. Programmet har medel reserverade för arbete 2023 till och med 2025

12 Definitioner

Cyberhot- En potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer

13 Övrigt

Styrgruppens medlemmar:

- Näringsminister- Fredrik Karlström
- LR IT- förvaltning och programmets beställare- Jani Sjölund
- LR ägarstyrning- Runa Tufvesson
- Sakkunnig- Andreas Parjus
- Åda VD- Christan Jansson
- Sakkunnig- Richard Boije
- Programledare Åsa Schmiedhofer

14 Referenser

Ref.nr.	Dokumentnamn, dokumentbeteckning
1	NIS2 https://eur-lex.europa.eu/eli/dir/2022/2555
2	ISO 27001- Ledningssystem - att arbeta systematiskt https://www.iso.org/standard/27001