MSB

Ansökan om projektmedel inom cybersäkerhet

Uppgiftsnamn	Uppgiftsvärde
Grunduppgifter	
Typ av organisation	Företag
Namn på sökande organisation	Lamm Consulting AB
Organisationsnummer	559355-2168
Postadress	Sibyllegatan 52 A
Postnummer	115 23
Postort	Stockholm
Land	Sweden
Kommun	Stockholms kommun
Litet eller medelstort företag	Ja
Har ert företag verksamhet i andra länder utanför EU/EES-området?	Nej
Har ni ägare/delägare eller kontrolleras företaget av aktörer utanför EU/EES-området?	Nej
Kontaktperson	
Förnamn	HANS
Efternamn	THORSEN LAMM
Telefonnummer	070-879 24 41
Mobiltelefonnummer	070-879 24 41
E-postadress	hans@lammda.se
Kontaktperson för projektet är även projektledare	Ja
Projektinformation	
Övergripande information	
Projekttitel svenska	NIS2 applicerat på aggregerade stödtjänster för el
Projekttitel engelska	NIS2 applied to energy grid
Projektsammanfattning svenska	

Projektet syftar till att analysera risker med aggregerade tjänster för elnätet. På grund av minskad rotationsenergi i samband med nedläggning kärnkraft och kraftig utbyggnad av sol och vind har det blivit allt svårare att upprätthålla en god frekvenskvalité. Frekvensen tillåts variera mellan 49,9 – 50,1 Hz. Ett exempel på stödtjänst är FCR-D som aktiveras när frekvensen understiger 49,9 Hz. Förbrukningsflexibilitet innebär att elanvändning i apparater styrs och förflyttas i tiden.
En del av lösningen är billiga IoT-lösningar riktade mot privatmarknaden. Genom att styra ett större antal små resurser såsom solceller, energilager, laddare och värmepumpar kan dessa tillsammans uppnå samma effekter som mycket stora anläggningar. Lösningen kallas aggregering och innebär att många privatpersoner på så vis kan agera på en marknad vilken omsätter sex miljarder kronor
Energibolag och nätägare vilka ansvarar för stora resurser förväntas ha hög cybersäkerhet . För mindre resurser så är kraven på cybersäkerhet lägre. Det är därför mycket troligt att

Uppgiftsnamn	Uppgiftsvärde
en angrepp mot elnätet sker via billiga IOT-lösningar. I Nederländerna har forskare redan rapporterat om riskerna, det är högst sannolikt att det samma även gäller här i Sverige. Förutom attacker mot energisystem, så kan även samma IoT lösningar användas för distribuerade överbelastningsattacker mot andra IT-system ansluta till Internet. Även andra risker kommer i mån av tid inkluderas såsom störningar på prissättning. NIS2 direktivet listar ett antal sektorer där berörda aktörer ska begära tillsyn av myndigheter . Styrning av energisystem via Internet borde därför involvera både Energimyndigheten och PTS. Med Sveriges inträde i NATO har vi även en skyldighet att tillhandahålla ett resilient energisystem. Projektet avser även analysera hur myndigheter hanterar risker som spänner över flera sektorer.	
Projektsammanfattning engelska	
Here's the translation to English: The project aims to analyze the risks associated with aggregated services for the power grid . Due to the decreased rotational energy related to the shutdown of nuclear power and the significant expansion of solar and wind energy, it has become increasingly difficult to maintain good frequency quality. The frequency is allowed to vary between 49.9 – 50.1 Hz. An example of a support service is FCR-D, which is activated when the frequency falls below 49.9 Hz. Consumption flexibility means that electricity usage in appliances is controlled and shifted in time. Part of the solution involves inexpensive IoT solutions aimed at the private market. By controlling a larger number of small resources such as solar panels, energy storage, chargers, and heat pumps, these can collectively achieve the same effects as very large facilities. This solution is called aggregation, allowing many individuals to participate in a market worth six billion kronor. Energy companies and grid owners responsible for large resources are expected to have high cybersecurity measures. For smaller resources, the cybersecurity requirements are lower. Therefore, it is highly likely that an attack on the power grid will occur through inexpensive IoT solutions. In the Netherlands, researchers have already reported on these risks, and it is very probable that the same applies here in Sweden. In addition to attacks on the energy system, the same IoT solutions can also be used for distributed denial-of-service attacks against other IT systems connected to the Internet. The NIS2 directive lists several sectors where relevant actors should seek oversight from authorities. Therefore, the governance of energy systems via the Internet should involve both the Swedish Energy Agency and PTS. With Sweden's entry into NATO, we also have an obligation to provide a resilient energy system. The project will also analyze how authorities manage risks that span multiple sectors	
Projektstart	2024-12-20
Projektslut	2025-02-12
Totalt sökt belopp i SEK	240 000
Utlysningsområde	
A. Säkerställa kunskap och kompetens inom cybersäkerhet: Området innefattar initiativ för att förbättra cybersäkerthetsmedvetenhet och utveckla säkrare digitala beteenden hos slutanvändare genom ökad kunskap om utmaningar och möjligheter inom cybersäkerhetsområdet.	X

Uppgiftsnamn	Uppgiftsvärde
B. Området innefattar utveckling av ledningssystem, processer, metoder och nyttjande av befintliga och nya teknologier för att förbätta och stärka beredskap inom informations- och cybersäkerhet samt skapa förståelse och medvetenhet kring risker vid bristfällig informations- och cybersäkerhet.	
C. Området avser initiativ som syftar till att bygga förmåga att möta nya regelverk och regulatoriska krav utifrån EU-reglering för ökad cybersäkerhet. Exempel på EU-reglering som avses är NIS2-direktivet, Cyberresiliensakten (CRA), Cybersolidaritetsakten (CSoA), Cybersäkerhetsakten, Förordningen för digital operativ motståndskraft (DORA) och AI-förordningen.	X

Bakgrund

Lamm Consulting AB verkar inom innovation och IT-säkerhet, och står som upphovsman bakom ett flertal patent. Ett av de tidiga patenten från 2003 handlar om hur kryptografiska nycklar används i Assa Abloys passersystem. Innan lösningen implementerades granskades den av ROMAB som för övrigt var en av lärarna vid Svenska Kraftnäts kurs i cybersäkerhet där Lamm Consulting deltog under våren 2024.
Via cybernode.se etablerades en kontakt med en utländsk tillverkare av OT/SCADA system som levererar lösningar till Siemens. Tillsammans med kunden och ett svenskt bolag verksamt inom energi har ett projektet startats.
Ett antal kontakter har initierats med Post och Telestyrelsen och Energimyndigheten avseende en granskning innan lösningen implementeras.

Projektmål

Det första arbetspaketet handlar om att kartlägga olika hot som aggregering av internetanslutna energiresurser innebär. Lamm Consulting har under våren 2024 genomgått en utbildning hos Svenska Kraftnät. Under Svenska Kraftnäts kurs i cybersäkerhet diskuterades olika modeller för att analysera hot. Med tanke på kopplingen till energisystem så kommer kartläggningen systemet att betraktas som ett OT/SCADA system snarare är en traditionell IT-sys

Relevans

Vid MSB:s cybersäkerhetskonferens den 14-15 oktober 2024 så efterlyste civilministern att myndigheter samarbetar. Internetansluten utrustning som påverkar energisystemet borde involvera minst två myndigheter, vidare så har MSB ett övergripande ansvar för samtliga myndigheter. Med Sveriges inträde i NATO har landet även en skyldighet att tillhandahålla ett resilient energisystem. Totalförsvaret kommer integreras i MSB som kommer byta namn till MSF 2026.

Projektplan

Namn på arbetspaket	Riskanalys

Kort beskrivning av arbetspaket

Det första arbetspaketet handlar om att kartlägga olika hot som aggregering av internetanslutna energiresurser innebär. Med tanke på kopplingen till det högkritiska

Uppgiftsnamn	Uppgiftsvärde
energisystem så kommer kartläggningen systemet att betraktas som ett OT/SCADA system . Då många av de ingående komponenterna även kan klassificeras så kommer standards såsom IoT Security Maturity Model: ISA/IEC 62443 beaktas.	
Andel av totalt sökt belopp (i %)	40
Namn på arbetspaket	Designdokument
Kort beskrivning av arbetspaket	
Det andra arbetspaketet handlar om att producera underlag för en “edge-computer” inför en granskning. En viktig funktion är hur denna komponent kan skydda energisystemet i befintliga installationer. Vi tror att Energimyndigheten bör involveras med stöd av PTS. Då endast en myndighet kan ge uppdrag till FRA eller FOI kommer vi även involvera någon större aktör inom energisektorn. Vår förhoppning är att delar av det granskade underlaget kan publiceras öppet.	
Andel av totalt sökt belopp (i %)	30
Namn på arbetspaket	Ledningsrapport
Kort beskrivning av arbetspaket	
Det tredje arbetspaketet handlar om regelefterlevnad. Förutom specifika krav såsom förkvalificering av stödtjänster kommer vi även beakta CRA och NIS2. Avseende NIS2 så avser vi analysera tre olika scenario. Det första handlar om att företagets omsättning och antal anställda. De andra handlar om företaget levererar en tjänst till någon aktör som står under tillsyn. Det tredje handlar om CRA och dess krav på att tillhanda uppdateringar avseende säkerhet under produktens livslängd.	
Andel av totalt sökt belopp (i %)	30
Leverabler	
Projektet kommer att leverera tre dokument. Det första dokumentet fokuserar på identifiering och analys av potentiella risker, vilket ger en tydlig översikt över hot och sårbarheter. Det andra dokumentet är en designlösning som adresserar dessa risker, vilket säkerställer en robust och säker struktur för våra tjänster. Det tredje dokumentet sammanfattar aktuella regulatoriska krav samt framtida krav kopplade till NIS2 och CRA. Det sista lämpar sig för beslutsfattare.	
Vilka långsiktiga effekter och nyttor förväntas projektet leda till?	
Lösningen kommer att hantera osäkra IoT-system som har implementerats innan NIS2 och CRA träder i kraft. Genom att offentligt publicera delar av vår granskade dokumentation, bidrar vi till kunskapsdelning och stödjer andra aktörer inom detta område. Genom att applicera regulatoriska krav på ett konkret fall hoppas vi att ge vägledning av typen "HUR", när det i dagsläget mest handlar om "ATT".	
Övriga åtaganden	
Har ni under de senaste 3 åren mottagit finansiellt stöd för utvecklingsprojekt?	Nej
Bilagor	
Bilaga	
?	arsredovisning - 559355-2168.pdf
Bilaga	
CV - Meritförteckning för personer som ska arbeta med projektet (PDF)	CV-hans-2024-11-11.pdf

Uppgiftsnamn	Uppgiftsvärde
Bilaga	
?	Registreringsbevis - 559355-2168.pdf
Bilaga	
Budget för projektet (Excel)	budgetmall-fstp-2024-09-12 1.xlsx
Bilaga	
Intyg om försumbart stöd/stöd av mindre betydelse (de-minimis) (PDF)	underskrivet_intyg.pdf
Sanningsförsäkran	
Härmed försäkras att ingen grund för uteslutning av ansökan föreligger i enlighet med artikel 136.1 och 141.1 i EU:s finansiella förordning	Ja
Härmed försäkras att uppgifterna som lämnats i denna ansökan är korrekta och riktiga, samt att sökanden åtar sig att meddela NCC-SE om något förändras under handläggningstiden	Ja

Dina personuppgifter behandlas enligt reglerna i allmänna dataskyddsförordningen, GDPR.

MSB behöver dina personuppgifter för att kunna behandla ditt ärende.

Support-Id: A04-A71