EFFEKTKARTLÄGGNING AV FINANSIERADE PROJEKT INOM UTLYSNINGEN BIDRAG TILL SMÅ OCH MEDELSTORA FÖRETAG FÖR KAPACITETSUPPBYGGNAD INOM CYBERSÄKERHET

Finansiellt stöd till tredje part (FSTP) inriktning kunskap och kompetens, beredskap och riskhantering, samt efterlevnad av EU-reglering

MYNDIGHETEN FÖR SAMHÄLLSSKYDD OCH BEREDSKAP (MSB)
SVERIGES NATIONELLA SAMORDNINGSCENTER FÖR FORSKNING OCH INNOVATION INOM CYBERSÄKERHET (NCC-SE)

attityd

NCC-SE
NATIONAL CYBERSECURITY COORDINATION CENTRE
SWEDEN

MSB
Myndigheten för samhällsskydd och beredskap

Sammanfattning

Bakgrund

Under perioden december 2024 till mars 2025 genomförde Myndigheten för samhällsskydd och beredskap (MSB), genom Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE), en riktad utlysning för att stärka cybersäkerhetsförmågan i Sverige. Utlysningen syftade till att mobilisera små och medelstora företag (SMF) genom att stödja utvecklingsprojekt inom tre strategiska kompetensområden: kunskap och kompetens, beredskap och riskhantering, samt efterlevnad av EU-reglering. Utöver det övergripande syftet var ambitionen att utlysningen skulle vara smidig med avseende på ansöknings- och rapporteringsprocessen. Vidare skulle stödet fungera som en katalysator i ekosystemet för kapacitetshöjande åtgärder inom cybersäkerhet med tydlig målgrupp: näringslivet små och medelstora företag. Attityd har under perioden juni – september 2025 haft i uppdrag av MSB att kartlägga effekterna av utlysningen. Rapporten riktar sig till aktörer inom cybersäkerhetsområdet, andra myndigheter och beslutsfattare som arbetar med liknande målgrupper och som kan dra lärdomar av utformningen och genomförandet av denna insats. Totalt beviljades stöd till 36 projekt av 180 inkomna ansökningar.

Metod

Denna rapport sammanfattar resultat och effekter av utlysningen baserat på dokumentstudier, enkätundersökning och djupintervjuer med deltagande företag. Samtlig datainsamling har genomförts av Attityd. Analys och reflektion har genomförts tillsammans med NCC-SE för att slutligen sammanfattas i denna rapport. Enkät och intervjuer har genomförts i nära anslutning till projektavslut, vilket betyder att kartläggningen har fokus på resultat och kortsiktiga effekter. Företag som ej beviljats medel har inte intervjuats, en målgrupp som kan vara relevant att undersöka framöver eller i kommande utlysningar. Mer långtgående effekter behöver följas upp längre fram, men företagens egna beskrivningar visar ändå på att projekten kan komma att bidra till kapacitetsuppbyggnad inom cybersäkerhet.

Resultat

Med avseende på att mobilisera näringslivet och nå SMF visar kartläggningen att utlysningen nått goda resultat. Utlysningen har i stor utsträckning attraherat företag inom IT-sektorn, många är mikroföretag och flertalet av dem är unga i organisation och/eller idé. Projekt har genomförts i samtliga tre målområden och majoriteten av projekten täcker in fler än ett målområde.

Kartläggningen visar att projektstödet haft en tydlig positiv inverkan, med konkreta resultat i form av nya tjänster, metoder och verktyg, samt stärkt medvetenhet och kapacitet inom cybersäkerhet. I enkätundersökningen framkommer att 90 % av företagen svarar ”mycket bra” på frågan om de har nått sina mål. 16 av 21 företag i enkätundersökningen uppger att de har tagit fram nya tekniska lösningar och 12 av 21 företag har tagit fram metoder och processer. Från intervjuerna framkommer att minst ett nytt företag har startats som en effekt av genomfört projekt.

Resultatet av enkätundersökningen visar på en rad olika kortsiktiga effekter.

Som exempel svarar företagen att projekten har bidragit ”väldigt mycket” till följande:

- ökad regelefterlevnad – 52 %
- ökad proaktivitet och förbättrad förmåga att detektera hot – 67 %
- ökad medvetenhet inom informations- och cybersäkerhet hos befintliga eller nya kunder – 57 %.

Dessa resultat indikerar att utlysningen redan har bidragit till kapacitetsuppbyggnad i linje med både EU:s och NCC-SE:s målsättningar.

När det gäller effekter på längre sikt visar enkätundersökningen att 76 % av företagen i hög grad har upplevt eller förväntas uppleva ett ökat kundförtroende och förbättrat anseende och 57 % att företaget har uppnått eller förväntas uppnå konkurrensfördelar på marknaden. På frågan om befintliga eller nya kunder har fått eller förväntas få en förbättrad motståndskraft genom ny eller vidareutveckling av produkt eller tjänst framkommer att 43 % instämmer i hög grad.

Att fullfinansieringen har varit en viktig framgångsfaktor i utlysningen framkommer i dokumentgranskning, enkätundersökning och intervjuer. Fullfinansieringen har möjliggjort deltagande för företag som annars inte har resurser att genomföra utvecklingsprojekt. Projektstödet har också fungerat som en katalysator för fortsatt utveckling och majoriteten av företagen har sökt (19 %) eller planerar att söka nya medel (57 %) t ex från Horisont Europa, programmet för ett digitalt Europa (DIGITAL) eller Vinnova.
Kartläggningen visar även att företagen ser behovet av att kroka arm med varandra och bygga hela leveranskedjor, varför nätverkande och erfarenhetsutbyte har setts som värdefullt. Företagens upplevelse är att detta hade kunnat vara än mer omfattande i utlysningen. Tanken var att Cybernoden, den nationella kompetensgemenskapen inom ramen för EU-projektet ECCC, skulle spela en central roll för såväl nätverkande som erfarenhetsutbyte, något som inte alla företag som fått finansiering uppmärksammat.

Ansökningsprocessen har enligt enkätsvar och intervjuer upplevts som relativt smidig, med tillgängligt stöd från NCC-SE. Samtidigt framkommer vissa tekniska hinder och behov av tydligare koppling mellan ansökan och rapportering, vilket pekar på förbättringspotential i strukturerna för ansökningsprocessen. En bättre teknisk struktur för ansökningar och rapportering skulle också effektivisera och öka möjligheten till uppföljningar likt denna rapport.

Innehållsförteckning

1 Bakgrund

EU har under de senaste åren valt att ta ett mer samlat grepp om cybersäkerhet. Genom finansiellt stöd ska unionen stärka sin konkurrenskraft, bygga kapacitet inom forskning och innovation samt utveckla kompetens för att möta nya säkerhetsutmaningar. Som ett led i detta etablerades europeiska kompetenscentrumet för cybersäkerhet (ECCC) i Bukarest, med ansvar för att utforma och hantera utlysningar inom programmen Horisont Europa och programmet för ett digitalt Europa (DIGITAL). ECCC samordnar även nationella samordningscenter (NCC) i varje medlemsland.

I Sverige har Myndigheten för samhällsskydd och beredskap (MSB) utsetts att vara nationellt samordningscenter enligt Europaparlamentets och rådets förordning (EU) 2021/887, även kallad CCCN-förordningen. Verksamheten bedrivs under namnet NCC-SE. NCC-SE har i uppdrag främja samarbete mellan akademi, näringsliv och myndigheter, stärka kontakterna mellan svenska och europeiska aktörer samt stödja ECCC i uppdraget att öka EU:s samlade cybersäkerhetsförmåga. I uppdraget ingår även att utforma och genomföra nationella satsningar för att bygga kapacitet i Sverige.

Mot denna bakgrund lanserade NCC-SE under slutet av 2024 en särskild satsning på finansiellt stöd till tredje part (FSTP). För att möjliggöra för NCC-SE att kunna lämna detta stöd togs förordningen om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning fram. I denna regleras bland annat under vilka förutsättningar stöd får lämnas och den skapar även möjlighet för NCC-SE att framöver kunna ge stöd till exempelvis lärosäten och kommuner. Satsningen inom FSTP har hittills riktat sig till små och medelstora företag, en målgrupp som lyfts fram i både EU-förordningen och den svenska cybersäkerhetsstrategin. Dessa företag anses samtidigt vara särskilt sårbara, då de ofta har begränsade resurser och kompetens för att hantera komplexa cyberrisker, men också särskilt viktiga, eftersom de utgör en central del av samhällsekonomin och spelar en viktig roll i innovationssystemet. Angrepp mot enskilda underleverantörer kan få spridningseffekter genom hela leveranskedjor, samtidigt som små företag kan driva fram nya lösningar som stärker samhällets samlade motståndskraft.

Utlysningen finansierades gemensamt med EU-medel inom DIGITAL och med nationella medel via MSB och Vinnova. Stödet omfattade upp till 600 000 kronor per projekt, med full kostnadstäckning och utan krav på medfinansiering. Inriktningen var bred, men strukturerad kring tre huvudområden: att stärka kunskap och kompetens, att förbättra beredskap och riskhantering samt att underlätta efterlevnad av nya EU-krav. På så sätt speglade satsningen både nationella behov och den europeiska utvecklingen. Samtidigt markerade den en ny arbetsmetod för MSB, då myndigheten för första gången gav direkt ekonomiskt stöd (de-minimis-stöd) till det privata näringslivet inom cybersäkerhet.

Behovet av en sådan satsning förstärktes av utvecklingen i omvärlden. Under 2023–2024 ökade cyberangreppen mot svenska aktörer markant, bland annat genom fler överbelastningsattacker mot myndigheter och samhällsviktig verksamhet. Samtidigt visade flera incidentrapporter på bristande grundförmåga i många organisationer. På europeisk nivå trädde nya regelverk i kraft, såsom NIS2-direktivet och Cyberresiliensförordningen, tillsammans med DORA-förordningen för finanssektorn och en kommande AI-förordning. Dessa regelverk skapar en ny kravbild som även mindre företag måste kunna hantera. Parallellt förändras den tekniska miljön snabbt med framväxten av AI, kvantteknologier, avancerade industriella system och digitala leveranskedjor, vilket både öppnar för innovation och ökar riskerna.

Genom att hålla utlysningen öppen för olika typer av projekt kunde NCC-SE fånga upp hela detta spektrum av behov. Bland de 180 inkomna ansökningarna valdes 36 projekt ut för finansiering. Dessa spände från utbildningsinsatser och övningar till utveckling av AI-baserade detektionssystem och förberedelser för kommande EU-certifieringar. Utlysningen FSTP 2024 blev därmed ett konkret bidrag till att stärka både Sveriges och EU:s oberoende förmåga och konkurrenskraft på cybersäkerhetsområdet, i linje med ambitionen om en säkrare digitalisering.

2 Om denna rapport

2.1 Syfte

Syftet med denna rapport är att analysera och sammanfatta de resultat och effekter som uppstått till följd av utlysningen, samt att belysa företagens upplevelse av ansöknings- och genomförandeprocessen. Syftet har varit att identifiera mönster, tendenser och lärdomar på en övergripande nivå, snarare än att bedöma varje projekts genomförande eller kvalitet.
Rapporten syftar också till att omsätta lärdomar till utvecklingsmöjligheter som kan ligga till grund för framtida utlysningar och insatser inom cybersäkerhetsområdet.

2.2 Frågeställningar

Effektkartläggningen har fokuserat på tre övergripande områden som tillsammans ger en bild av hur projektstödet har fungerat, vilka resultat det genererat och hur det upplevts av de deltagande företagen:

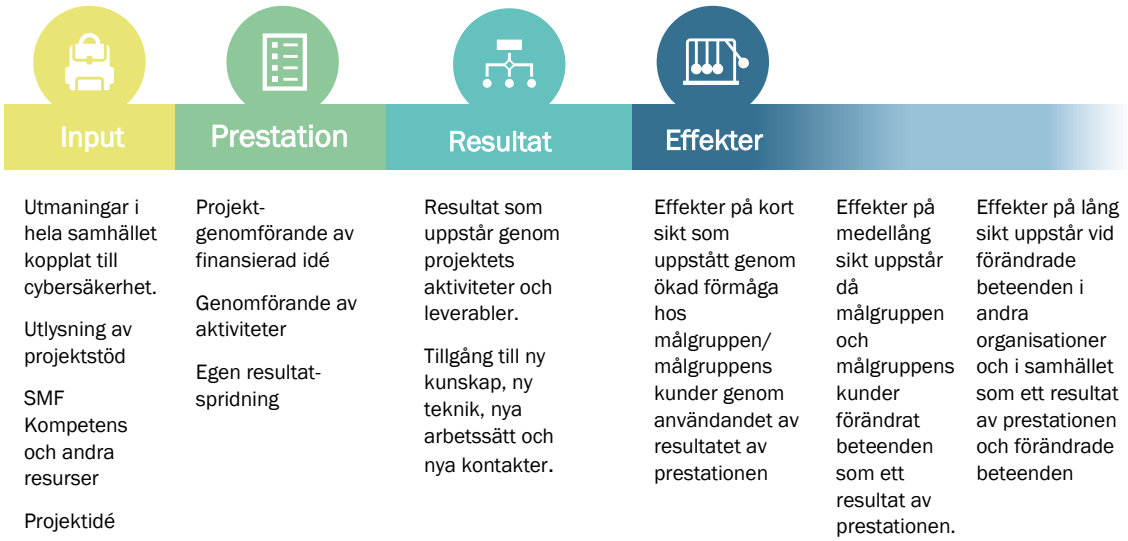
1. Projektresultat och effekter
   Hur har projektmedlen fördelats och vilka typer av företag har nåtts? Vilka konkreta resultat har projekten genererat, och vilka direkta och indirekta effekter har uppstått i företagens verksamheter och hos deras kunder?
2. Lärdomar och fortsatt utvecklingspotential
   Vilka framgångsfaktorer och hinder har identifierats under projektens genomförande? Vilka insikter kan tas vidare för att stärka framtida utlysningar och insatser inom cybersäkerhetsområdet?
3. Upplevelse av ansökningsprocessen och stödet från NCC-SE
   Hur har företagen upplevt ansökningsförfarandet, rapporteringskraven och kontakten med NCC-SE? Vilka förbättringsområden kan identifieras för att skapa lärande och utveckling?

2.3 Analytisk ram: Theory of Change

För att strukturera analysen av projektresultat och effekter har kartläggningen utgått från en förenklad modell av Theory of Change (ToC)1. ToC är en vedertagen metod för att beskriva hur en insats förväntas leda till önskade förändringar, genom att tydliggöra sambandet mellan insatsens resurser, aktiviteter, direkta resultat, effekter och långsiktig påverkan.
I denna kartläggning har ToC tillämpats för att:

- Identifiera förväntade effekter enligt utlysningens syfte och målområden.
- Samla in och analysera faktiska resultat från projekten i relation till dessa mål.
- Analysera förutsättningar för långsiktig påverkan, såsom ökad motståndskraft, förbättrad regelefterlevnad och stärkt kundrelation.

[1] https://www.theoryofchange.org/what-is-theory-of-change/toc-background/toc-origins/



FIGUR 1 PROJEKTENS FÖRÄNDRINGSLOGIK

2.4 Omfattning och metod

Effektkartläggningen har genomförts med en mixed methods-ansats, där både kvalitativa och kvantitativa metoder kombinerats för att fånga projektens resultat och upplevda effekter. Analysen har strukturerats utifrån en förenklad Theory of Change-modell, vilket möjliggjort en systematisk bedömning av hur projektstödet omsatts i konkreta resultat och förväntad påverkan. All datainsamling är genomförd av Attityd på uppdrag av MSB.

Metod	Beskrivning
Dokumentstudie	Samtliga 36 projekt har lämnat in slutrapporter som analyserats systematiskt. Rapporterna innehåller information om projektens genomförande, leverabler, måluppfyllelse samt upplevda hinder och framgångsfaktorer. De innehåller även reflektioner kring utlysningen och kontakt med NCC-SE. Se bilaga 1 Deltagande företag
Enkät	En webbenkät har utformats utifrån insikter från dokumentstudien och skickats till en kontaktperson i respektive projekt. Syftet har varit att samla in kvantitativa data om projektens resultat, effekter, samt upplevelsen av ansökningsprocessen, rapportering och stöd. Totalt besvarades enkäten av 21 av de 36 projekten, dvs. en svarsfrekvens på 58 %. Se bilaga 2 Enkätfrågor
Kvalitativa djupintervjuer	Djupintervjuer har genomförts med ett urval av företag för att fånga mer nyanserade perspektiv på projektens effekter, både inom den egna organisationen och gentemot kunder. Intervjuerna har också belyst lärdomar och framtida utvecklingsbehov. Totalt har nio intervjuer genomförts. Se bilaga 3 Frågeguide
Analys	Analysen har genomförts iterativt under kartläggningens gång, med löpande tematisering av insamlat material. Slutligen har en sammanvägd analys gjorts av både kvantitativa och kvalitativa data för att identifiera mönster, avvikelser och lärdomar. Ett möte genomfördes tillsammans med NCC-SE för att gemensamt analysera det framkomna resultatet. Den gemensamma analysen bidrar till att tillgodogöra sig resultat och analyser och lägger därmed grunden till arbetet med framtida utlysningar.

TABELL 1 METOD OCH KÄLLOR

2.5 Avgränsningar

Denna kartläggning har fokuserat på att analysera utlysningen som helhet och de samlade effekterna av projektstödet. Rapporten utvärderar inte de enskilda projektens aktiviteter eller resultat i detalj, utan bygger på företagens egna redogörelser i slutrapporter, enkätsvar och intervjuer. Syftet har varit att identifiera mönster, tendenser och lärdomar på en övergripande nivå, snarare än att bedöma varje projekts genomförande eller kvalitet.

Det innebär att rapporten inte innehåller en djupgående granskning av tekniska lösningar, metodval eller resultat i respektive projekt. Fokus har istället legat på att förstå hur utlysningen som insats har fungerat, vilka typer av företag som nåtts och vilka effekter som uppstått i bredare bemärkelse.

2.5.1 Eventuella begränsningar i materialet

Resultaten i denna kartläggning bygger i huvudsak på företagens egna redogörelser i slutrapporter, enkätsvar och intervjuer. Det innebär att analysen baseras på självskattade upplevelser och effekter, vilket kan påverkas av subjektiva faktorer såsom företagens förväntningar, tolkningar och kommunikationsförmåga.
Kartläggningen har inte inkluderat en oberoende granskning av de tekniska eller organisatoriska lösningar som utvecklats inom respektive projekt. Det innebär att resultaten inte verifierar effekterna på detaljnivå, utan ger en övergripande bild av hur utlysningen som insats har fungerat och vilka mönster som kan urskiljas. Vidare genomfördes kartläggningen kort tid efter att projekten avslutats, vilket innebär att långsiktiga effekter ännu inte fullt ut kunnat observeras eller bedömas. De resultat som presenteras bör därför ses som preliminära indikationer på riktning och potential, snarare än slutgiltiga utfall.

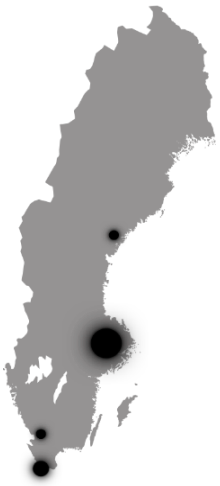
3 Resultat

3.1 Fördelning av stöd med avseende på företag och projektinriktning

Utlysningen hade som ambition att mobilisera små och medelstora företag, både i rollen som behovsägare och som leverantörer, inom tre definierade kompetensområden. Totalt genomförde 36 företag projekt (se Bilaga 1 Deltagande företag) inom ramen för utlysningen.

Region	Antal
Region Stockholm	17
Region Skåne	6
Region Västernorrland	2
Region Halland	2
Region Blekinge, Jämtland Härjedalen, Jönköpings län, Sörmland, Värmland, Västerbotten, Örebro län, Östergötland samt Västra Götalandsregionen	1

TABELL 2 FÖRDELNING AV PROJEKT PER REGION



FIGUR 2 FÖRDELNING AV PROJEKT PER REGION

Dokumentstudien visar att 13 av Sveriges 21 regioner finns representerade bland beviljade projekt. Kartläggningen visar också på en tydlig geografisk koncentration till Region Stockholm, där 17 företag återfinns. Därefter följde Region Skåne med 6 deltagande företag. I Halland och Västernorrland deltog två företag vardera, medan övriga regioner representerades av ett eller inget företag per region.
Ur ett storleksperspektiv dominerades deltagandet av mikroföretag (färre än 10 anställda) och små företag (10–49 anställda). Endast ett företag klassificerades som medelstort (50–249 anställda). Både dokumentanalys och intervjuer visar att en stor andel av företagen inom IT-sektorn är unga med avseende på marknads- och/eller organisatorisk mognad.

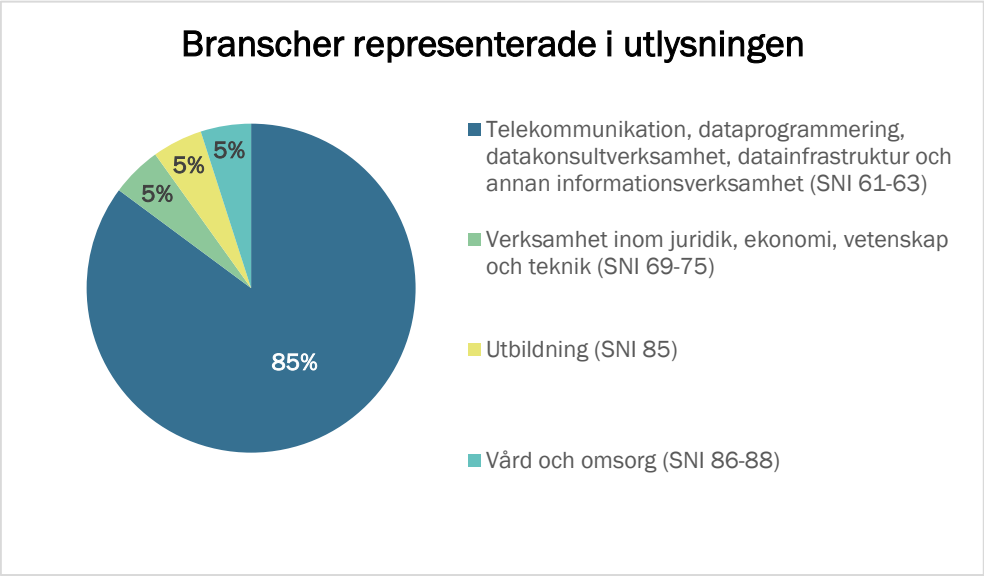


DIAGRAM 1 FÖRETAGENS BRANSCHTILLHÖRIGHET, DÄR 85% ÅTERFANNS INOM SNI-KOD 61–63. N=21

Enkätundersökningen visar att företagen kategoriserade sig under fyra olika SNI-koder.
Den största andelen, 85 %, tillhörde sektorn för information och kommunikation (SNI 61–63). Övriga deltagande företag återfanns inom juridik, ekonomi och tekniska konsulttjänster (SNI 69–75), utbildning (SNI 85) samt vård och omsorg (SNI 86–88), vilka vardera utgjorde 5 % av det totala antalet.

3.1.1 Tidigare erfarenheter av utlysningsmedel och stödets påverkan på genomförandet

Av de nio företag som intervjuades inom ramen för utvärderingen saknade majoriteten tidigare erfarenhet av att ansöka om projektstöd både generellt och specifikt inom EU-programmen Horisont Europa samt DIGITAL. FSTP-utlysningen kom därmed att fungera som en första introduktion till denna typ av offentlig finansiering. En bidragande faktor till detta, enligt både dokumentstudien och intervjuresultatet, var att utlysningen erbjöd full finansiering, vilket av de flesta företag lyftes fram som avgörande för deras deltagande.
Under de fördjupade intervjuerna framkom att flertalet företag redan hade idéer som väl matchade utlysningens syfte och inriktning. Ett mindre antal företag identifierade däremot möjligheter först i samband med att utlysningen kom dem till känna.
Enkätsvaren visar att stödet upplevdes som mycket relevant och väl anpassat till företagens individuella behov. Svaren koncentrerades till de högre nivåerna på bedömningsskalan, vilket indikerar att projektstödet i ”hög grad”, eller ”mycket hög grad”, uppfattades som svarande mot de utmaningar och behov som företagen stod inför. Vidare visar enkäten att de åtgärder som genomförts inom ramen för projekten i stor utsträckning inte skulle ha realiserats utan det ekonomiska stödet. Detta resultat understryker stödets betydelse för att möjliggöra genomförandet av projekten. Intervjuerna bekräftar denna bild, där flera företag uttryckligen framhåller finansieringen som en avgörande faktor för att projektet kunde genomföras.

> "Det var en lyckträff – rätt tidpunkt och rätt finansiering."

3.2 Projektens syfte, inriktning och mål

I enkätundersökningen uppgav totalt 67 % av företagen att deras huvudsakliga mål var att stärka sitt externa erbjudande, vilket indikerar att projekten i stor utsträckning betraktades som en möjlighet att öka konkurrenskraften och leverera förbättrat värde till marknaden eller till specifika målgrupper.

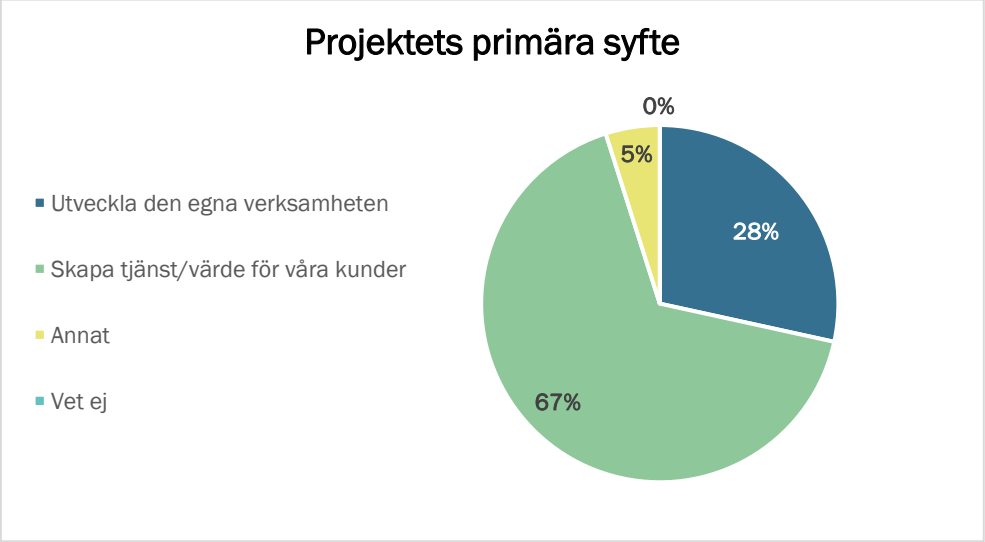


DIAGRAM 2 PRIMÄRT SYFTE MED PROJEKTEN UR FÖRETAGENS PERSPEKTIV. N= 21

Fördelningen mellan dessa områden bekräftas i dokumentstudien av projektens slutrapporter, där samtliga projekt är representerade.
Dokumentstudien visar också på att kundvärde i denna kontext kan innebära:

- utveckling av nya tjänster eller produkter,
- förvärv av ny kunskap under projektets gång som kommer kunder till nytta,
- förstärkt säkerhet inom den egna organisationen
  med syfte att skapa trygghet och värde för kunden.

En mindre, men ändå betydande, andel företag (28 %) uppgav att projektets syfte främst var att ”utveckla den egna verksamheten”. Ett litet antal företag valde alternativet "annat". Enligt fritextsvaret kan detta förklaras med att företag skiljer på utbildning som genomfördes kostnadsfritt till andra SMF under projektgenomförandet och att efter projekttiden erbjuda det som en tjänst.

3.2.1 Val av målområde och huvudinriktning på projekten

Vid ansökan om projektstöd fick företagen ange ett eller flera målområden som sökt projekt skulle bidra till, med fokus på att stärka cybersäkerhetsförmågan i samhället. De tre definierade målområdena var:

A. Säkerställa kunskap och kompetens inom cybersäkerhet
B. Beredskap och hantering av cybersäkerhetsrelaterade risker
C. Förmåga att efterleva krav från EU-reglering inom cybersäkerhetsområdet

Enligt dokumentstudien fördelade sig företagens val enligt följande:

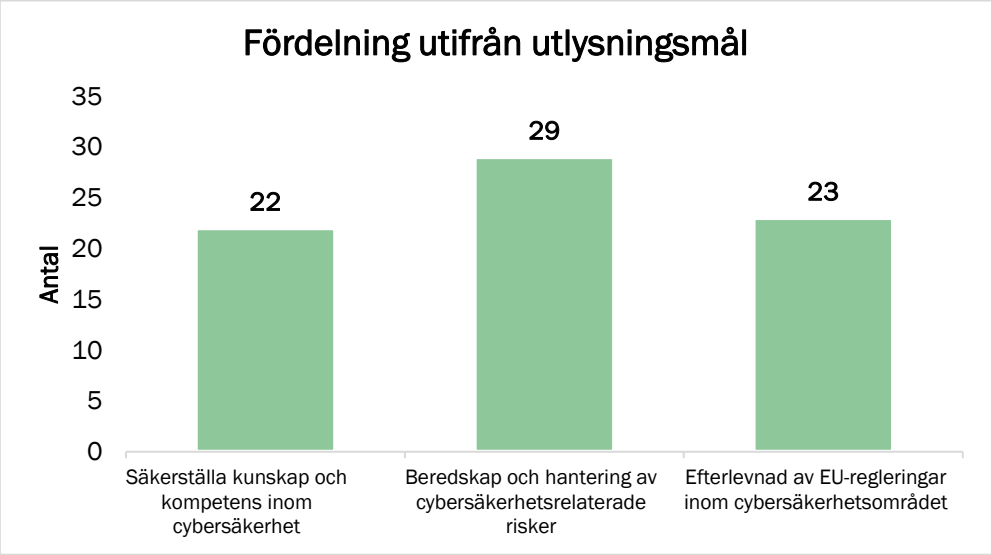


DIAGRAM 3 FÖRDELNING AV ANTALET PROJEKT INOM RESPEKTIVE UTLYSNINGSMÅL. N = 36

Dokumentstudien visar också att två tredjedelar av företagen har genomfört projekt som bidrar till mer än ett målområde, vilket är viktigt att beakta vid tolkning av statistiken. Detta mönster speglar att cybersäkerhet är ett komplext och tvärgående område där olika insatser ofta samverkar, vilket också är anledningen att NCC-SE valde att inte avgränsa till att välja ett enskilt mål i FSTP 2024.

Projektens tyngdpunkt: att stötta organisation, organisering och arbetssätt

Utöver de olika målområdena har kartläggningen, utifrån projektens syftesbeskrivning samt slutrapporter, kategoriserat projektens huvudinriktning med avseende på organisation, teknik och beteende. Vilken kategori projektet kopplats till är baserat på det område som varit mest centralt för respektive projekt. Majoriteten av projekten har haft fokus på organisatoriska aspekter och arbetssätt. Följande tre kategorier har identifierats:

- Organisation/arbetssätt: Inkluderar utveckling av processer och rutiner samt tekniska komponenter (system, tjänster) som stödjer dessa.
- Teknik: Omfattar nya tekniska lösningar och system.
- Människa/beteende: Avser insatser med fokus på psykologi, pedagogik och beteendeförändring.

Denna kategorisering tydliggör att projekten inte enbart varit teknikorienterade, utan även inkluderat organisatoriska och mänskliga dimensioner av cybersäkerhetsarbete.

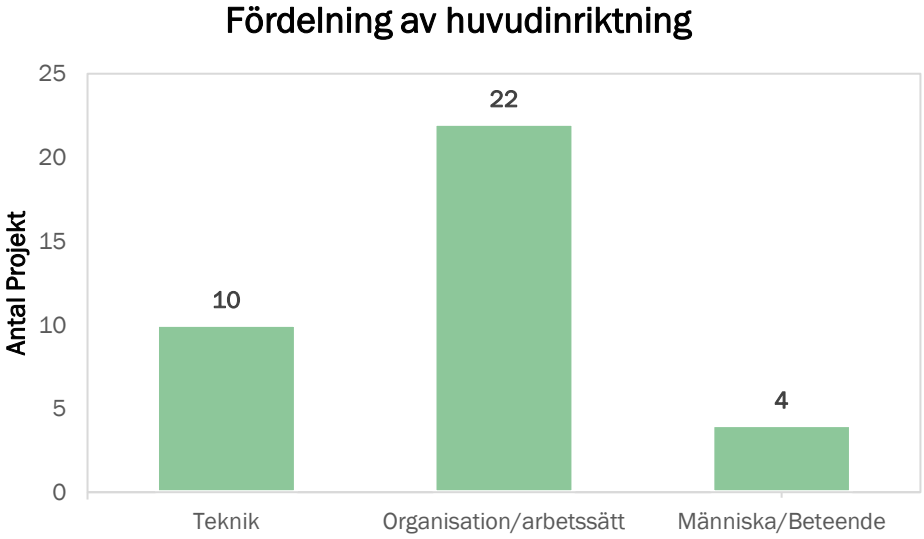


DIAGRAM 4 SAMMANSTÄLLNING AV PROJEKTENS HUVUDINRIKTNING N=36

I både slutrapporter och intervjuer framhåller flera företag att mänskligt agerande är avgörande för samhällets cybersäkerhet. Kunskap och träning i kombination med tekniska verktyg lyfts fram som centrala komponenter, vilket också återspeglas i den överlappning som finns mellan målområdena i Diagram 3 och kan även skönjas vid identifiering av projektinriktningarna.

3.3 Projektresultat

Detta kapitel sammanfattar projektens resultat kopplat till prestationen i modellen över förändringslogik som introducerades i kapitel 2.4. Projektens resultat innefattar måluppfyllnad, utfall av projektens aktiviteter, vad som levererats i projekten, samt om och hur resultaten spridits.

3.3.1 Måluppfyllnad

Enligt enkätundersökningen (n = 21) bedömer företagen att projektmålen i stor utsträckning har uppnåtts. Över 90 % av respondenterna angav att målen uppnåtts ”mycket bra”, medan knappt 10 % svarade att målen nåtts ”ganska bra”. Denna fördelning indikerar ett starkt genomslag och god måluppfyllelse inom ramen för utlysningen.

90%

Anser att de uppnått sina mål ”mycket bra”

3.3.2 Projektens leverabler

I enkätundersökningen fick företagen ange vilken eller vilka typer av leverabler som projektet resulterat i. Resultaten visar att projekten lett till en bredd av konkreta leverabler som gett goda effekter redan under eller kort efter projekttiden, se kapitel 3.4.1. Tekniska lösningar har högst förekomst följt av nya metoder och processer, utbildning och presentationsmaterial.

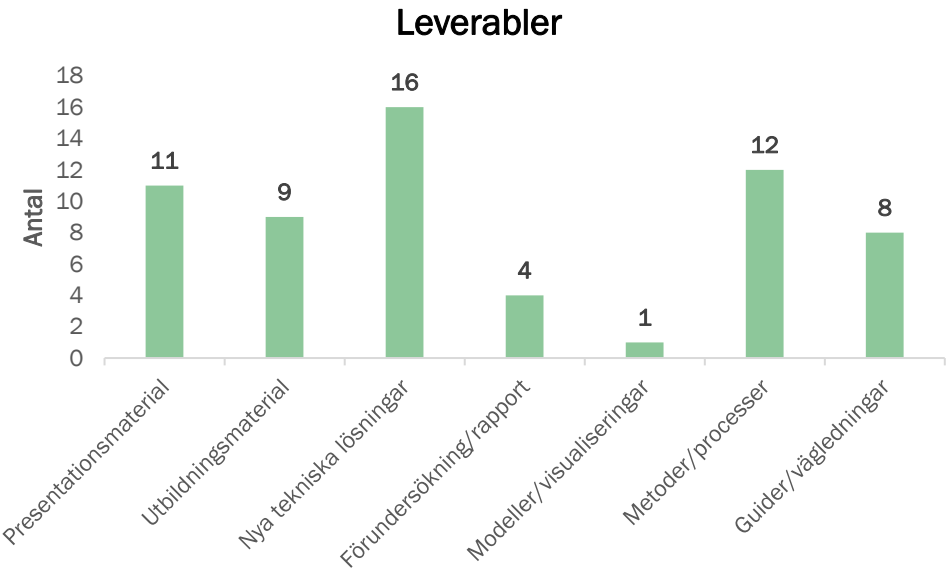


DIAGRAM 5 VAD HAR PROJEKTET LEVERERAT/TAGIT FRAM? FLERVALSFRÅGA, N=21

I dokumentstudien av slutrapporter och i intervjuer berättar företagen att projektet omfattat kunskapshöjande insatser både internt och till externa parter. Flertalet projekt har levererat intern utveckling av metoder, processer samt implementering av ledningssystem. Största andelen av projekten har arbetat med nya tekniska lösningar där flertalet företag anger att resultatet finns som öppen källkod eller kostnadsfria lösningar. Flera företag har valt att stärka sin egen verksamhet, och därigenom sitt kunderbjudande, genom penetrationstester och åtgärder för att minska sårbarheter i befintliga system.

Ur dokumentstudien och i intervjuer kan kartläggningen finna att 13 företag beskriver att projektet resulterat eller kommer att resultera i utveckling av nya tjänster. Vidare berättar 8 företag om vidareutveckling av befintliga tjänster.

3.3.3 Resultatspridning

Enkätundersökningen visar att en tydlig majoritet, 90 %, av företagen har spridit material och projektresultat till aktörer utanför det egna projektet.
Vidare visar resultatet av dokumentstudien samt intervjuer att projekten har spridit resultat i en bredd av kanaler som sociala medier, evenemang, och i sin marknadskommunikation. Detta innebär en ökad medvetenhet samt kunskapshöjning både inom och utanför egna organisationen. Det framkommer i dokumentstudien att fortsatt spridning med stor sannolikhet kommer att ske, utifrån de leverabler som tagits fram och hur de kommer att nyttjas framgent.

FIGUR 3 FORTSATT SPRIDNING AV PROJEKTRESULTAT

3.4 Effekter

Projektstödet har genererat flera positiva effekter hos de deltagande företagen, i relation till de målområden som definierades i utlysningen. I följande delkapitel delas projekteffekter på kort och lång sikt. Effekterna är främst observerbara på kort sikt då denna kartläggning genomförts nära projektavslut. I både slutrapporter och intervjuer har kartläggningen fångat upp att det finns tydliga indikationer på att företagen har både ambition, kapacitet och avsikt att ta resultaten vidare efter projekttiden. I rapportens sista kapitel förs resonemang om hur arbetet skulle kunna fortsätta för att nå de långsiktiga effekterna både i denna utlysning och kommande.

3.4.1 Projekteffekter kopplat till målområden, kort sikt

Enkätresultatet visar att en majoritet av företagen uppger att medvetenheten om informations- och cybersäkerhet inom den egna organisationen har ökat som ett direkt resultat av projektet. Enkätsvaren visar att de flesta har tillägnat sig ny kunskap och ökad förståelse för säkerhetsrelaterade frågor. 67 % svarar ”väldigt mycket” och 19 % ”ganska mycket” Detta indikerar att projektet haft en betydande inverkan på hur dessa frågor hanteras och prioriteras i verksamheten.

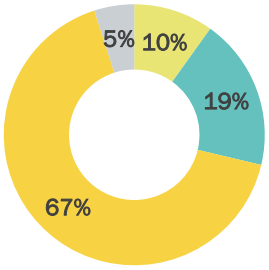


DIAGRAM 6 ÖKAD MEDVETENHET OM INFORMATIONS/CYBERSÄKERHET INOM ORGANISATIONEN. N=21

Vidare framgår att en tydlig majoritet av företagen identifierat nya utvecklingsbehov kopplade till informations- och cybersäkerhet. Respondenterna angav i stor utsträckning att projektet bidragit ”väldigt mycket” (67 %) till att synliggöra områden där ytterligare insatser krävs. Detta indikerar att det finns behov att fortsätta utvecklingen inom området. Endast ett fåtal företag rapporterade att projektet endast ”till viss del” synliggjort nya utvecklingsbehov.

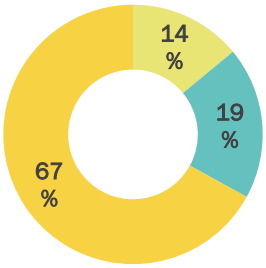


DIAGRAM 7 UPPLEVELSE AV ATT HA SYNLIGGJORT NYA UTVECKLINGSBEHOV RELATERADE TILL CYBERSÄKERHET, N=21

Resultatet visar att en majoritet av företagen upplevde en ökad förmåga att arbeta mer strukturerat med cybersäkerhet. 57 % anger att de ökat sin förmåga ”väldigt mycket”, 10 % anger ”ganska mycket” och 24 % upplever att de ökat sin förmåga ”till viss del”.

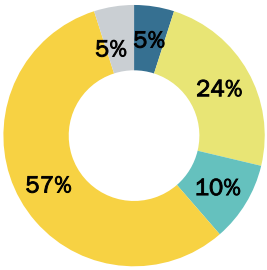


DIAGRAM 8 UPPLEVELSE AV ÖKAD FÖRMÅGA ATT ARBETA MER STRUKTURERAT MED INFORMATIONS-/CYBERSÄKERHET. N=21

En klar majoritet av företagen rapporterar också en ökad proaktivitet och förbättrad förmåga att detektera och hantera cybersäkerhetsrisker. Enkätsvaren visar att denna förmåga har stärkts ”ganska mycket” (24 %) eller ”väldigt mycket” (67 %), vilket tyder på att projektet haft en direkt inverkan på det förebyggande och reaktiva cyber-säkerhetsarbetet. Vissa företag angav att förmågan endast ökat till viss del, vilket antyder att effekten varierat beroende på företagens förutsättningar och projektinriktning.

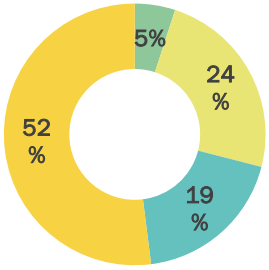


DIAGRAM 9 UPPLEVELSE AV ATT HA ÖKAT PROAKTIVITETEN OCH/ELLER FÖRMÅGAN TILL ATT DETEKTERA OCH HANTERA CYBERSÄKERHETSRISKER. N=21

Projektstödet har även haft en positiv effekt på företagens förmåga att uppfylla krav relaterade till regelverk och standarder, såsom GDPR och NIS2. De flesta företag (57 %) uppger att deras efterlevnad förbättrats ”väldigt mycket”. 14 % anger ”ganska mycket” och 24 % anger ”till viss del” Detta indikerar att stödet bidragit till att stärka företagens kapacitet att hantera regulatoriska krav och integrera dessa i sin verksamhet.

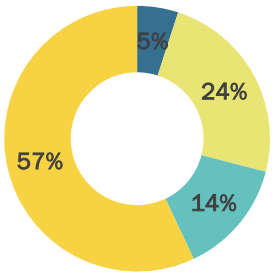


DIAGRAM 10 UPPLEVELSE AV ATT HA FÖRBÄTTRADE MÖJLIGHETER/LÖSNINGAR TILL EFTERLEVNAD AV REGLER OCH STANDARDER, SÅSOM GDPR OCH NIS2. N=21

Slutligen visar resultaten att en tydlig majoritet av företagen upplevt – eller förväntar sig att uppleva en ökad medvetenhet hos sin kundbas som en följd av projektet. De flesta respondenter (52 %) angav att denna medvetenhet ökat ”väldigt mycket”. Detta tyder på att insatser inom produkt- och tjänsteutveckling haft en positiv inverkan på kundernas förståelse och engagemang i frågor som rör informations- och cybersäkerhet. Från dokumentstudien och intervjuer kan konstateras att det relativt höga antalet svarsalternativ med "till viss del" 24 % kan kopplas till att flera av de deltagande företagen är unga mikroföretag eller att nya affärsområden utvecklats inom projekten som ännu inte lanserats på marknaden. I vissa fall har dock kundmedverkan skett under projekttiden, vilket kan ha bidragit till ökad medvetenhet även utan att en färdig produkt lanserats.

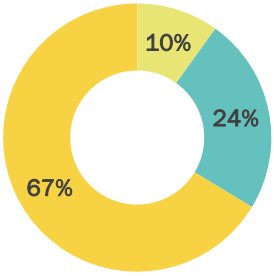


DIAGRAM 11 UPPLEVELSE AV ÖKAD MEDVETENHET HOS BEFINTLIGA ELLER NYA KUNDER GENOM NY ELLER VIDAREUTVECKLING AV PRODUKT/TJÄNST. N=21

3.4.2 Andra kortsiktiga effekter

Utöver de direkta effekterna på företagens säkerhetsarbete och tekniska kapacitet har projektstödet genererat ett antal indirekta och kompletterande effekter. Dessa effekter omfattar spridning inom och utanför organisationen, etablering av nya nätverk, samt ökad benägenhet att söka ytterligare projektmedel. Resultaten bör ses som en indikation på projektets bredare påverkan på målgruppen med avseende på mobilisering av SMF som en viktig komponent i ekosystemet för kapacitetshöjning inom cybersäkerhet.
Vid intervjuerna framkommer att flera företag rapporterar ytterligare effekter, såsom:

- genom projektet har verifiering validering av juridiska aspekter kunnat genomföras i företagets tekniska lösning. Produkten och tjänster kopplat till produkten lyfts ut i nytt bolag.
- projektet har lett till synliggörande av nya behov och nya målgrupper vilket lett till att flera företag har eller kommer att **etablera nya affärsområden och tjänster**,
- projektresultat har kunnat användas för att **bygga förtroende** i marknadskommunikation och säljprocesser,
- **tillgång till nya arenor för nätverkande** samt kontakter med myndigheter, akademiska aktörer och potentiella kunder. Som exempel blev 9 av de deltagande företagen medlemmar i Cybernoden under projekttiden.

Dokumentstudien samt intervjuerna visar att nästan samtliga projekt har formulerat en tydlig plan för fortsatt utveckling, vilket tyder på att FSTP-medlen i många fall fungerat som en katalysator. Särskilt stark potential identifieras inom teknisk fördjupning, marknadsförberedelse samt fortsatt kunskapsspridning.

En stor andel av företagen uppger i enkäten att de redan har sökt, eller planerar att söka, nya projektmedel efter avslutat FSTP-projekt. Projektstödet har alltså fungerat som en katalysator för fortsatt utveckling då majoriteten av företagen har sökt (19 %) eller planerar att söka nya medel (57 %) till exempel från Horisont Europa, DIGITAL eller Vinnova. Knappt en fjärdedel av företagen har inte några planer på att söka ytterligare medel, 5 % är osäkra.

DIAGRAM 9 FÖRETAGENS AMBITION ATT SÖKA NÄSTA NIVÅ AV STÖD, TILL EXEMPEL HORISONT EUROPA, DIGITAL, VINNOVA ELLER LIKNANDE. N=21

Sammantaget tyder svaren i enkäten på ett utbrett intresse för fortsatta satsningar och en vilja att bygga vidare på de erfarenheter och framgångar som genererats inom ramen för projektet. Denna indikation förstärks också av intervjuerna där företagen kopplar utlysning och genomförandet av projekten till att de hittat nya utvecklingsområden och fått direkta effekter som lett dem framåt både med avseende på utveckling, marknadsintroduktion och nya relevanta kontakter.

3.4.3 Projekteffekter kopplat till målområden, lång sikt

Då projekten nyligen avslutats, baseras bedömningen av långsiktiga effekter på företagens egna uppskattningar och förväntningar. Det är därför viktigt att tolka resultaten som preliminära indikationer snarare än definitiva utfall. Trots detta ger svaren en värdefull inblick i hur projektstödet upplevs ha påverkat företagens strategiska utveckling och motståndskraft mot cybersäkerhetsrisker

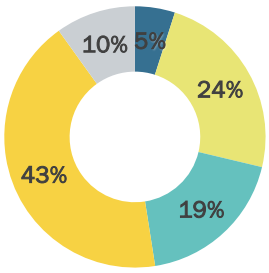


DIAGRAM 10 UPPLEVELSE AV EN STARKARE FÖRMÅGA ATT HANTERA NYA OCH KOMPLEXA CYBERHOT SOM FÖLJD AV PROJEKTET. N=21

Enkäten visar att företagen bedömer att deras organisatoriska motståndskraft har stärkts påtagligt som ett resultat av projektet. Svaren visar en tydlig förskjutning mot de högre nivåerna på skalan, där de flesta företag angav att motståndskraften förväntas öka ”väldigt mycket” (43 %). 19 % svarade ”ganska mycket” och 24 % placerade sig i mellankategorin ”till viss del”, Endast ett fåtal angav låg påverkan. Sammantaget indikerar detta en övervägande positiv uppfattning om projektets bidrag till ökad robusthet mot cybersäkerhetsrisker på längre sikt.

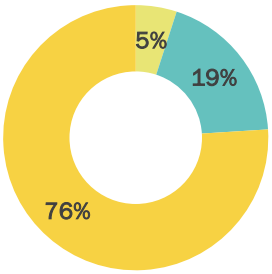


DIAGRAM 14 UPPLEVELSE AV ATT HA ÖKAT ANSEENDE HOS SINA KUNDER SOM FÖLJD AV PROJEKTET. N=21

Vidare uppger en klar majoritet av företagen anser att projektstödet haft, eller förväntas ha, positiva effekter på lång sikt i form av förbättrat anseende och stärkt kundrelation. Svaren domineras av de högre kategorierna, där 76 % svarade att det bidragit ”väldigt mycket” och 19 % svarade ”ganska mycket”. Detta tyder på att projektet bidragit till ökad tillit och förtroende från marknaden och att effekterna sträcker sig bortom tekniska förbättringar och även omfattar strategiska värden såsom varumärkesstyrka och kundlojalitet.

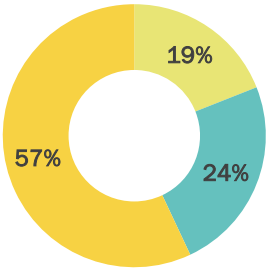


DIAGRAM 15 UPPLEVELSE AV ATT UPPNÅ KONKURRENSFÖRDELAR PÅ MARKNADEN SOM FÖLJD AV PROJEKTET. N=21

57 % av företagen uppger att projektstödet har påverkat deras konkurrenskraft ”väldigt mycket”. Det är dock värt att notera att 24 % av företagen angav att effekten endast varit till viss del. Från intervjuerna kan konstateras att det delvis kan förklaras med att flera av de deltagande företagen har en bit kvar innan de är etablerade på marknaden, eller att nya affärsområden utvecklats som ännu inte lanserats på marknaden. Flertalet projekt har haft fokus på den interna verksamheten vilket också kan spegla en lägre förväntad påverkan på både anseende och konkurrenskraft.

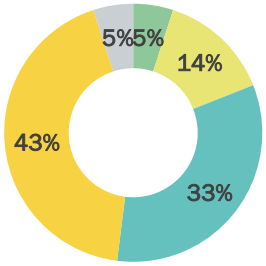


DIAGRAM 16 FÖRBÄTTRAD MOTSTÅNDSKRAFT HOS BEFINTLIGA OCH/ELLER NYA KUNDER GENOM TJÄNST/PRODUKT. N=21

Företagen bedömer att deras produkter och tjänster, utvecklade inom ramen för projektet, kommer att ha bidragit till att stärka kundernas förmåga att stå emot cybersäkerhetsrisker. Majoriteten av svaren återfinns i kategorierna ”ganska mycket” (33 %) och ”väldigt mycket” (43 %), vilket tyder på att projektstödet inte enbart haft interna effekter, utan även förstärkt företagens externa erbjudanden. Vissa företag angav till viss del, och ett fåtal rapporterade mycket begränsad omfattning, vilket visar att effekten varierar mellan företag beroende på projektets inriktning och kundrelationer.

Väldigt mycket | Ganska mycket | Till viss del | I mycket begränsad omfattning | Inte alls | Ej relevant/vet ej

3.5 Ansökning, rapportering och stöd av NCC-SE

Företagens upplevelse av ansökningsprocessen, rapportering och det stöd som tillhandahållits av NCC-SE har överlag varit positiv, med några få inslag som indikerar att det finns förbättringspotential. Processerna har i stort upplevts som tydliga och hanterbara, men tekniska och kommunikativa utmaningar har förekommit. Av de intervjuade företagen fick merparten information om FSTP-utlysningen via LinkedIn eller genom kommunikation, direkt eller indirekt via företagens kontakter, från Cybernoden.

3.5.1 Upplevelse av ansökningsprocess och rapportering

Enligt enkätundersökningen upplevde majoriteten av företagen att ansöknings-, rapporterings- och utbetalningsmomenten fungerade väl. De flesta respondenter angav att dessa delar fungerade i ganska hög eller mycket hög grad, vilket tyder på att hanteringen av stödet generellt sett upplevdes som tillfredsställande. En mindre andel företag angav ”ganska låg grad” av smidighet i processen, vilket indikerar att det finns utrymme för förbättring.

Företagen bedömde att målen och kriterierna för stödet var tydligt kommunicerade. En övervägande majoritet angav att dessa var mycket tydliga, medan övriga respondenter angav ganska tydliga. Informationen om stödet upplevdes också som tillgänglig och användbar – de flesta företag angav att de i ganska hög eller mycket hög grad haft tillgång till tillräcklig information. Enstaka företag svarade vet ej, vilket antyder att informationsspridningen i stort varit effektiv, men inte heltäckande.

När det gäller kontakten med NCC-SE visar resultaten i enkäten att samtliga svarande företag upplevde bemötandet som gott. Över 90 % angav att det varit mycket lätt att komma i kontakt med NCC-SE, medan en mindre andel (under 10 %) angav att det varit ganska svårt. På samma sätt uppgav över 90 % att de i mycket hög grad fått den hjälp de behövde, medan en mindre andel svarade i ganska hög grad eller varken eller.

90%

Uppger att det både varit lätt att komma i kontakt med NCC-SE och att de fått den hjälp de behövde.

Dokumentstudien och intervjuer visar däremot på att upplevelsen av kontakten med NCC-SE varierade. Några företag beskrev en god och kontinuerlig dialog, medan andra upplevde svårigheter att få svar, särskilt under projektets inledande fas.

Enkätens fritextsvar samt intervjuer visar att flertalet företag upplevde tekniska problem med MSB:s e-tjänst, otydlig terminologi samt bristande koppling mellan ansökan och slutrapportering. En tydligare vägledning och förbättrad funktionalitet efterfrågas inför kommande utlysningar.

3.6 Erfarenheter och framtida behov

3.6.1 Framgångsfaktorer och goda erfarenheter

Enligt enkätundersökningen upplevde majoriteten av företagen att projektet genomfördes framgångsrikt och enligt plan. Framgången tillskrivs framför allt det tydliga och lättillgängliga upplägget för ansökan och projektgenomförande. Den enkla strukturen bidrog till att företagen snabbt kunde formulera en konkret projektidé och skapa en genomförbar plan, vilket ligger i linje med NCC-SE:s målsättning att erbjuda ett stöd som är lätt att ta del av – särskilt för aktörer med begränsad erfarenhet av offentliga projektmedel. Under intervjuerna framkom att den korta projekttiden, i kombination med en tydlig ansökningsstruktur, drev företagen att fokusera och avgränsa sina insatser. Detta upplevdes som positivt och bidrog till att projekten höll en hög grad av måluppfyllelse. Flera företag lyfte fram det interna engagemanget som en nyckelfaktor – med motiverade team och tydlig ansvarsfördelning som möjliggjorde effektivt genomförande.

3.6.2 Hinder och mindre bra erfarenheter

Trots den övergripande positiva bilden identifierades även ett antal utmaningar. Den begränsade projekttiden upplevdes som pressande av flera företag, särskilt i förberedelsefasen. Tidsramen försvårade möjligheten att nå ut till målgrupper, genomföra bredare spridningsinsatser och skapa långsiktig påverkan. Flera företag uttryckte att en något längre projektperiod hade kunnat ge bättre verkan och mer hållbara resultat.

> ”Tidspress, vi hade kunnat sprida ut projektet över några månader till, och förmodligen få bättre verkan.”

Tillgången till rätt kompetens inom cybersäkerhet lyftes också som en utmaning både i slutrapporter och i intervjuer, särskilt bland mindre företag. Flera projekt arbetade med avancerade teknologier, såsom AI i, kombination med cybersäkerhet, vilket innebar att de befann sig i teknikens framkant utan tydliga föregångare att inspireras av. Den snabba utvecklingen inom området, tillsammans med nya regelverk och riktlinjer som implementeras löpande, ställer höga krav på både teknisk och juridisk förståelse. Här finns ett behov av att framtida utlysningar är i takt med aktuella policyförändringar för att minska hinder under genomförandet.
Slutligen uttryckte flera företag en önskan om att få dela sina resultat mer aktivt – exempelvis genom erfarenhetsutbyte, gemensamma presentationer eller konferenser. Många upplevde att deras projekt genererat värdefulla insikter och lösningar som hade kunnat komma fler aktörer till nytta om fler möjligheter till spridning hade erbjudits. Ur både dokumentstudie och samtal med NCC-SE framkommer att ett antal aktiviteter har skett inom detta område. Projekten har också själva spridit sina resultat. Resonemang om spridning med avseende på roller och ansvar finns i nästa kapitel - Lärdomar samt Slutsatser och rekommendationer.

3.6.3 Företagens lärdomar

I både dokumentstudie och intervjuer kan kartläggningen ringa in flera viktiga lärdomar som kan bidra till utvecklingen av framtida insatser.

3.6.3.1 Företagens lärdomar kopplade till projektens genomförande

Flera företag lyfte fram vikten av att planera in tillräcklig tid och flexibilitet i projekten med avseende att förstå, följa och tillämpa komplexa regelverk som NIS2 och AI-förordningen.

> ”En lärdom är att det krävs tydlig prioritering och dedikerad tid för att driva komplexa regelverk som NIS2 och EU:s AI-förordning från teori till praktisk tillämpning.”

Flera företag beskrev marknaden för cybersäkerhetslösningar som omogen, vilket innebär ett stort behov av utbildning, medvetandegörande och stöd i att navigera nya krav. Projekten har bidragit till att öka förståelsen för marknadens behov och potential, och flera företag uttryckte att de fått nya insikter om hur stort behovet faktiskt är.

> ”Vi har lärt oss mer om marknaden och behovet som kommer för den här typen av lösningar, det som sticker ut är hur stort behovet är!”

3.6.3.2 Företagens lärdomar kopplade till utlysningens utformning och process

Genom att erbjuda full finansiering och ett tydligt ramverk har utlysningen möjliggjort deltagande för aktörer som annars inte hade haft resurser att genomföra utvecklingsprojekt. Att ge stöd till SMF med avseende att mobilisera för kapacitetsuppbyggnad inom cybersäkerhet har träffat rätt även ur företagens perspektiv då konkurrenskraft med stor sannolikhet leder till effekter på sikt.

> ”Att denna typ av projekt ger en möjlighet för mindre/nya bolag att öka sin konkurrenskraft”

Andra viktiga lärdomar som kan dras ur resultatet av de kvalitativa intervjuerna samt dokumentstudien är att företagen har varierad bild av relationen med NCC-SE. Flera hade bilden av att utlysningen skulle innebära ett nära samarbete med NCC-SE och ge företagen en ökad möjlighet att få kontakter och på sikt bli leverantörer till MSB. Företagen lyfte även att de hade förväntan på att projektens resultat skulle spridas av NCC-SE.

Det är viktigt att notera att detta var en utlysning av utvecklingsbidrag och det ligger utanför utlysningens syfte att medverka i projekten, inleda en affärsmässig relation eller marknadsföra de lösningar projekten tagit fram. MSB som myndighet varken kan eller får ta en sådan roll. Det som kan utvecklas till kommande utlysningar är kommunikationen med företagen som beviljas projektstöd för att tydliggöra dessa roller och därmed ge goda förutsättningar till en korrekt förväntansbild.

3.6.4 Företagens framtida behov

Företagen som deltagit i FSTP-utlysningen ser ett stort värde i att delta i framtida utlysningar. Ur projektens slutrapporter kan vi ringa in ett antal önskemål och områden. Det framkommer bland annat att det i kommande utlysningar finns utrymme att bygga vidare på de resultat som åstadkommits i genomförda projekt. Här avses både att ta ursprunglig projektidé till nästa steg samt att fånga nya utvecklingsbehov som framkommit som ett indirekt resultat av projektet. Företagen lyfter att behovet inom cybersäkerhetsområdet är stort, både med avseende på förståelsen för vikten av ett aktivt cybersäkerhetsarbete, vilka regelverk som finns att förhålla sig till, samt behovet av stöd för att organisera arbetet i organisationen. Det framkommer även att det är viktigt att stärka kapacitet och kompetens i hela samhället och att möjliggöra tillämpning av teknik och regelverk i den egna organisationen samt hos företagens kunder.

Det finns en tydlig önskan om att utlysningarna fortsatt ska vara tillgängliga för små aktörer och vara kopplade till strategiska behov i såväl Sverige som EU. Företagen lyfter även i dokumentstudien att framtida utlysningar bör synkroniseras med implementering av nya regelverk. Vidare framkommer att utlysningarna bör vara tematiskt fokuserade, det bör skiljas på kapacitetsuppbyggnad i form av innovation och utveckling och rena utbildningsinsatser.

I såväl dokumentstudie som intervjuer framkommer att ytterligare samverkan skulle öka företagens bidrag till kapacitetsuppbyggnad.

4 Slutsatser och rekommendationer

Nedan följer våra slutsatser och rekommendationer. I dialog med NCC-SE har vi reflekterat över resultatet och identifierat ett antal områden som kan vara värdefulla att fortsätta utveckla till kommande utlysningar. Det är tydligt att NCC-SE har arbetat för att redan nu skapa goda förutsättningar för lärande och utveckling för att nå effekter av FSTP 2024 och kommande utlysningar. Analysen inkluderar, tydliggörande av roller och ansvar, stöd till mikroföretag, mätbara effektmål och uppföljning.

4.1 Tydliggörande av roller och ansvar

En aspekt som återkommit i kartläggningen handlar om behovet av tydligare roller och ansvar mellan NCC-SE och de sökande företagen. Det handlar dels om kontakt och kommunikation under projektets gång, dels om NCC-SE:s roll avseende spridning av projektresultat och marknadsföring av deltagande företag. Såväl intervjuer med företag som med NCC-SE visar på att NCC-SE under processens gång har fångat upp utmaningar som uppstått och visat en vilja att utveckla arbetssättet på ett positivt sätt. En rekommendation framgent blir att fortsätta tydliggöra vem som gör vad, vilket stöd som finns att tillgå och vad som förväntas i olika delar av processen.

4.2 Stöd till mikroföretag

En stor andel av de företag som beviljats stöd i utlysningen är mikroföretag och flertalet av dem är unga i organisation och/eller i sin idé, flera med ett starkt innovationsfokus, vilket innebär stor potential – men också ett behov av stöd för att kunna ta nästa steg och på sikt generera effekter. Det kan handla om olika typer av stöd. Ett område som företagen själva lyfter är att de ser behov av att kroka arm med andra företag för att bygga hela leveranskedjor, varför nätverkande och erfarenhetsutbyte har setts som värdefullt. Företagens upplevelse är att detta hade kunnat vara än mer omfattande i utlysningen. Tanken var att Cybernoden, den nationella kompetensgemenskapen inom ramen för EU-projektet ECCC, skulle spela en central roll för såväl nätverkande som erfarenhetsutbyte, något som inte alla företag som fått finansiering uppmärksammat. Positivt är att utlysningen renderade nio nya medlemmar till Cybernoden (tre av företagen var redan medlemmar), men det kan konstateras att 24 företag inte valt att gå med som medlemmar och därmed gått miste om möjligheten att nätverk, samverka och dela sina erfarenheter, som de också har efterfrågat. En rekommendation blir därför att än tydligare synliggöra Cybernoden som plattform för samverkan, erfarenhetsutbyte och lärande.

4.3 Mätbara effektmål och uppföljning

Synpunkter kring ansökningsprocessen har tagits emot och lett till förbättringar, vilket är positivt. Vissa utmaningar kvarstår i och med de tekniska lösningar som står till förfogande. För att ytterligare stärka möjligheten att följa upp projekten kan det vara värdefullt att arbeta med tydliga effektmål redan i ansökningsskedet. Genom att utforma projekten så att både kortsiktiga resultat och effekter samt långsiktiga effekter kan mätas, skapas bättre förutsättningar för att förstå hur de påverkar beteenden, förmågor och i förlängningen samhället i stort. Många projekt har ett tydligt resultatfokus, men för att effekterna ska bli bestående behöver resultaten också tas vidare och omsättas i praktiken. En rekommendation är därför att arbeta med tydliga effektmål, både kortsiktiga och långsiktiga, redan i utlysningen, i själva ansökningsförfarandet samt i slutrapporteringen. Ett konkret exempel är att företagen får uppge antal nya företag samt antal nya produkter och tjänster i slutrapporteringen.

För att fånga de långsiktiga effekterna av projekten ser vi ett värde i att följa upp projekten över tid – exempelvis efter ett, tre och fem år. Genom att analysera vilka företag som har fortsatt utvecklas och bidragit till kapacitetsuppbyggnad, kan man få viktig kunskap om vad som fungerar och vad som ger effekt. Det är särskilt intressant att jämföra olika utlysningar och se hur justeringar i upplägg har påverkat resultaten. Redan i den andra utlysningen har NCC-SE tagit vara på lärdomar från den första, vilket visar på ett aktivt och reflekterande arbetssätt.

4.4 Avslutningsvis

Det arbete som NCC-SE redan har gjort visar på engagemang och en vilja att utvecklas. Genom att fortsätta bygga vidare på de insikter som framkommit i kartläggningen finns goda möjligheter att förstärka effekterna av både nuvarande och framtida satsningar. Det handlar inte om att förändra allt, utan snarare om att förfina och förstärka det som redan fungerar – och att fortsätta vara lyhörd för målgruppens behov.

Bilagor

Bilaga 1 Deltagande företag och projekt

Företag	Projektsammanfattning
Actensa Group	Projektet syftar till att utveckla en ResilienceBot, en AI-baserad lösning som stödjer kris- och kontinuitetshantering. ResilienceBot ska möjliggöra snabbare och effektivare hantering av störningar genom att automatisera och optimera befintliga planer och processer. Genom marknads- och teknisk validering avser projektet säkerställa att lösningen möter marknadens behov och förbättrar förmågan att hantera och återhämta sig från allvarliga cyberincidenter.
Atsec information security	Projektet adresserar sårbarhetshantering inom ramen för nya EU-regelverk såsom Cybersäkerhetsakten och tillhörande genomförandeförordning EUCC. Projektet innebär att utveckla processer och verktyg för att möta kraven i dessa regelverk.
Bitfront	Projektet syftar till att utveckla ett öppet verktyg för att skapa en exakt och tillförlitlig SBOM (Software Bill of Materials) för C/C++-applikationer. Projektet avser utveckla metoder och verktyg för säkrare digitala leveranskedjor på ett innovativt och praktiskt sätt.
Certezza	Projektet syftar till att skapa en vägledning som stödjer verksamhetsutövare i övergången till kvantsäkra algoritmer. Projektet adresserar behovet av ökad kunskap och beredskap inom cybersäkerhet kopplat till kryptering, med fokus på att hjälpa verksamheter att möta kommande regulatoriska krav och stärka sin informationssäkerhet.
ChangeAbility	Projektet syftar till att skapa ett metodstöd för beteendebaserad cybersäkerhet, som underlättar design, implementation och effektmätning av organisatoriska säkerhetsåtgärder. Metodstödet ska bygga en brygga mellan teknik och människa för att stärka medvetenhet och säkra beteenden, i linje med EU:s krav och NIS2-direktivet.
Clever Collaboration Group	Projektet CyberReady SME syftar till att stärka svenska SME:ers cybersäkerhet genom en digital verktygslåda för utbildning, regulatorisk efterlevnad och krishantering. Projektet adresserar viktiga cybersäkerhetsutmaningar och utbildar SME om regelverk som NIS2 och Cybersäkerhetsakten.
Daniel Eriksson Teknik	Projektet syftar till att stärka företagets cybersäkerhet genom att uppgradera befintliga brandväggar och intrusion detection systems (IDS). Målet för projektet är att implementera avancerade system med stöd för AI-baserad hotdetektering och realtidsförebyggande åtgärder för att skydda företagets nätverk och kundernas data mot cyberattacker.
Dizparc Secured	Projektet syftar till att erbjuda kostnadsfria utbildningar för små och medelstora företag samt IT-leverantörer i norra Mellansverige. Utbildningarna adresserar praktisk cybersäkerhet, inklusive hotbildsanalyser, incidenthantering och kravställning för säkra digitala lösningar.
Ension	Projektet syftar till att utveckla en metod och modell för att analysera och dokumentera design av riskhanteringsåtgärder enligt cybersäkerhetslagen. Genom att integrera standarder som ISO 27001 och ISO 61508 i en modellbaserad arbetsprocess, adresserar projektet behovet av cybersäkerhet by design.
GovSec Sweden	Projektet syftar till att förbättra cybersäkerhetsmedvetandet genom teoretisk och praktisk utbildning i svensk cyberlagstiftning och EU:s regelverk. Utbildningen riktar sig till aktörer inom samhällsviktig verksamhet enligt NIS-direktivet. Fokusområden inkluderar hotbildsanalys, cyberhygien, kryptering, AI-hot, samt skydd av kritisk infrastruktur. Praktiska övningar i riskhantering, gap-analyser och planering inför cyberkriser avser stärker deltagarnas förmåga att hantera aktuella och framtida cybersäkerhetsutmaningar.

Gridheart	Projektet syftar till att stödja Managed Service Providers (MSP) i att förstå och efterleva NIS2-direktivet samt stärka cybersäkerheten hos SMF. Genom behovsanalyser, workshops och utveckling av utbildningsmaterial avser projektet adressera NIS2-krav och bidrar till att höja säkerheten. Resultatet av projektet förväntas bidra till nya säkerhetstjänster och ökad beredskap mot hot som ransomware hos SMF.
INTERNETWORKING STOCKHOLM	Projektet syftar till att utveckla en AI-driven tjänst för cybersäkerhets-utvärdering som stödjer svenska företag att uppfylla NIS2-direktivet. Plattformen avser erbjuda en interaktiv bedömning av användares cybersäkerhetsmognad, baserad på AI-modeller som ger konkreta rekommendationer för regelefterlevnad och säkerhetsförbättringar. Tjänsten avser stärka företagens motståndskraft mot cyberhot och bidrar till en säkrare digital infrastruktur.
ITSL solutions	Projektet syftar till att utveckla en teknisk referensarkitektur och rekommendationer för SaaS-leverantörer som hanterar sekretessbelagda uppgifter inom offentlig sektor. Genom samarbete med ledande molnleverantörer analyseras säkerhetskrav från OSL, PDL, GDPR och AI-Act. Referensarkitekturen demonstreras i en proof-of-concept lösning för säker digital kommunikation, vilket stärker offentlig sektors förmåga att möta lagkrav och säkerhetsutmaningar.
Leyr Health	Projektet syftar till att stärka cybersäkerheten inom hälso- och sjukvården genom att utveckla förbättrad integrationslösning för journalsystem. Genom penetrationstester, utbildning och spridning av kunskap om säker utveckling avser projektet adressera viktiga cybersäkerhetsutmaningar och bidrar till ökad patientsäkerhet och stärkt informationssäkerhet i kritisk infrastruktur.
Medoma	Projektet syftar till att utveckla och dokumentera processer samt implementera tekniska säkerhetsåtgärder för att möta kraven i NIS2 och AI-förordningen. Projektet stärker cybersäkerheten i hälso- och sjukvården genom robusta rutiner, teknisk förbättring och spridning av lärdomar vilket förväntas bidra till en nationell säkerhetsstandard och i förlängningen ökad patientsäkerhet.
Menacit	Projektet syftar till att utveckla utbildningsmaterial för att hjälpa organisationer att förbättra säkerheten i Kubernetes-baserade IT-plattformar. Kursmaterialet kommer att vara fritt tillgängligt, vilket förväntas stärka kompetens inom cybersäkerhet för systemadministratörer och IT-säkerhetsspecialister och bidrar till ökad säkerhet i samhällskritiska tjänster.
MPQ Software	Projektet syftar till att utveckla ett verktyg för informationssäkerhet som riktar sig till små och medelstora företag. Verktyget möjliggör ISO27001-certifiering genom att erbjuda stöd för riskanalys, säkerhetsåtgärder, lagövervakning och incidentrapportering.
Netgraph Sverige	Projektet syftar till att förstärka säkerheten i Netgraphs molnbaserade lösningar för gästnätverk genom att implementera processer för säkerhetsövervakning och incidenthantering i enlighet med NIS2-direktivet. Dessutom inleds dokumentation och rutinarbete för ISO27001-certifiering. Projektet adresserar säkerhetsrisker kopplade till gästnätverk och stärker både Netgraphs och deras kunders motståndskraft mot cyberhot.
Nordic Foresights	Projektet syftar till att utveckla ett erfarenhetsbaserat utbildningspaket för att stärka förmågan hos ledningar i små och medelstora företag, kommuner och ideella organisationer att hantera utpressningsattacker. Utbildningen fokuserar på handlingsberedskap, krisledning och kommunikation, och är utformad för att ge ledningspersoner utan teknisk IT-bakgrund rätt verktyg för att möta cybersäkerhetsrelaterade utmaningar.
Observit	Projektet syftar till att stärka cybersäkerheten inom kollektivtrafikens övervakningssystem genom implementering av ett certifieringsklart ledningssystem enligt ISO 27001 och efterlevnad av NIS2-direktivet. Genom strukturerad dokumentation, tekniska säkerhetskontroller och utbildning av personal bidrar projektet till höjd säkerhet för kritisk infrastruktur och fungerar som en modell för andra leverantörer i sektorn.

Okatima	Projektet syftar till att designa och producera en prototyp av ett mobilt escape room med cybersäkerhet som tema. Spelet kombinerar digitala och fysiska pussel och riktar sig till unga, med fokus på att öka medvetenheten om cybersäkerhet och digital hygien. Spelet och tillhörande utbildningsmaterial skapas under öppen licens.
Perimed	Projektet syftar till att utveckla och implementera processer och arbetssätt för att stärka cybersäkerheten i medicintekniska produkter för perifer cirkulationsmätning. Genom att harmonisera med standarder som IEC 81001-5-1 och genomföra sårbarhetsanalyser bidrar projektet till säkrare vård och uppfyllande av regulatoriska krav, vilket i slutändan förväntas bidra till ökat skydd av patientdata och kritisk sjukvårdsinfrastruktur.
QNOVA SYSTEMS	Projektet HYBRID syftar till att säkerställa cybersäkerheten i QNOVAs molntjänst för avtalshantering, särskilt anpassat för offentlig sektor och reglerade industrier. Genom penntester, granskning och intern utbildning höjs säkerhetsnivån för att möta krav från regelverk som NIS2 och DORA. Projektet förväntas stärka beredskapen mot cyberhot och förbättrar skyddet av känslig avtalsinformation.
Safestate	Projektet syftar till att utveckla en användarvänlig kundportal för svenska SMF som erbjuder översikt över cybersäkerhetstjänster, larmrapporter och rekommenderade åtgärder. Genom att integrera alla säkerhetstjänster på en plats bidrar projektet till ökat engagemang och bättre hantering av hot, vilket förväntas stärker småföretagares cybersäkerhet och därigenom bidra till Sveriges totalförsvar.
Scionova	Projektet syftar till att stärka organisationens förmåga att hantera cybersäkerhetsrisker genom att bygga kompetens inom sårbarhetshantering. Utbildningsmoduler utvecklas för att höja säkerhetskompetensen hos olika roller i företaget och integreras i utvecklings- och leveransprocesser.
Secure by me	Projektet syftar till att utveckla och distribuera en handbok samt erbjuda utbildningar i systematisk informationssäkerhet riktade till svenska kommuner. Genom att ge kommuner tillgång till praktiska verktyg och kunskap förväntas projektet stärka kommuners förmåga att bedriva ett robust och långsiktigt informationssäkerhetsarbete.
Softjoy	Projektet syftar till att utveckla ett IT-system för att analysera cybersäkerheten för svenska .se-domäner, med fokus på e-postsäkerhet och DNS-resiliens. Genom att identifiera brister i säkerhetsstandarder och presentera konkreta rekommendationer, stärker projektet Sveriges förmåga att hantera cyberhot. Resultaten, inklusive en nationell cybersäkerhetsrapport, förväntas bidra till en säkrare digital miljö för både offentliga och privata aktörer.
Stratsys	Projektet syftar till att utveckla ett integrerat ledningssystem som ger små och medelstora företag en tydlig översikt över cybersäkerhetsrisker och efterlevnad av EU-regelverk såsom NIS2, DORA och Cyberresiliensakten. Genom att samla och analysera data från interna system och leverantörs-kedjor möjliggör systemet effektivare riskhantering och uppfyllande av regelverkskrav. Plattformen bidrar till förbättrad resiliens och stärker cybersäkerhetsberedskapen hos användarna.
Stellar Capacity	Projektet syftar till att genomföra en pilot för cybersäkerhetsutbildning riktad till alumner från Stellar Capacity med bakgrund inom digitalt ledarskap och AI. Utbildningen genomförs i två format: digitalt och på plats. Syftet är att stärka deltagarnas förmåga att identifiera hot, fatta informerade beslut och implementera cybersäkerhetsstrategier i sina organisationer. Utbildningen inkluderar interaktiva övningar, praktiska scenarier och live hacking-demonstrationer.
Storegate	Projektet syftar till att integrera tjänstelegitimationen SITHS eID i Storegates molntjänst för att erbjuda säkrare inloggning och fildelning för offentlig sektor. Genom denna integration adresseras behovet av att använda högsäkerhetslegitimationer i kritiska verksamheter, vilket förväntas stärka cybersäkerheten och uppfylla krav från ny reglering.

Stretch Care	Projektet syftar till att stärka Stretch Care AB:s kvalitetssystem genom att anpassa verksamheten till NIS2- och CRA-direktiven samt implementera ISO 27001. Genom en omfattande GAP-analys och åtgärder adresseras krav från nya EU-regleringar, vilket förväntas förbättra säkerheten för känslig patientinformation som hanteras via bolagets vårdsystem och medicintekniska produkter.
Teleservice Skåne	Projektet syftar till att stärka företagets förmåga att hantera cybersäkerhetsangrepp genom kontinuitetsplanering, krisövningar och utbildningar för medarbetare. Projektet inkluderar även penetrationstester och en analys av nya regulatoriska krav som NIS2. Insatserna kommer att förbättra både företagets och kundernas säkerhet samt bidra till ökad motståndskraft mot cyberhot.
Urban Hippo	Projektet syftar till att utveckla en SaaS-tjänst som hjälper företag att identifiera, mäta och jämföra kritiska KPI:er inom cybersäkerhet. Genom att möjliggöra benchmarking och prioritering av de mest relevanta KPI:erna, avser projektet adressera små och medelstora företags behov av säkerhetsinsatser där de ger störst effekt. Lösningen förväntas stärka cybersäkerhet samt förbättra motståndskraften mot cyberhot som ransomware.
Vigili	Projektet syftar till att vidareutveckla en IT-säkerhetsutbildning för företag och organisationer, med fokus på förbättrad pedagogik och psykologiska principer för att stärka inlärning och beteendeförändringar. Genom extern expertis och tekniska förbättringar adresserar projektet behovet av effektiva, skalbara utbildningar som stärker små och medelstora företags cybersäkerhet. Resultaten från pilottester med företag kommer att användas för att optimera tjänsten och avser stärka Sveriges cybersäkerhetskultur.
West Code solutions	Projektet syftar till att anpassa revisions- och incidenthanteringsverktyget Isap för att stödja efterlevnad av NIS2-direktivet. Genom att utveckla funktioner för riskhantering och systematiskt säkerhetsarbete adresserar projektet behovet av användarvänliga verktyg som stöttar små och medelstora företag i att uppnå regulatoriska krav.
31173 Services	Projektet syftar till att etablera ett ledningssystem för informationssäkerhet (LIS/ISMS) enligt ISO27001 samt en virtuell SOC (Security Operations Center) för hantering av cybersäkerhetsincidenter. Projektet adresserar den ökande frekvensen av cyberattacker mot bolagets och kundernas infrastruktur och stärker företagets förmåga att hantera hot och följa EU:s regulatoriska krav, inklusive NIS2.

Bilaga 2 Enkätfrågor

Bilagan kan inhämtas genom att kontakta NCC-SE via mailadressen: ncc-se@msb.se

Bilaga 3 Frågeguide intervjuer

Bilagan kan inhämtas genom att kontakta NCC-SE via mailadressen: ncc-se@msb.se

Nina Engdahl
Projektledare
054-777 06 01
nina@attitydikarlstad.se
attitydikarlstad.se