HANDLINGSPLAN FÖR EN STARKARE CYBERSÄKERHETSINDUSTRI

i Stockholmsregionen

Region Stockholm

Handlingsplan för en starkare cybersäkerhetsindustri
RS 2024-0587

Handlingsplan under Näringslivs- och tillväxtstrategi för Stockholmsregionen
RS 2020-0780

November 2024

Grafisk form och produktion: Luxlucid

Inledning

HANDLINGSPLANEN FÖR EN STARKARE CYBERSÄKERHETS-INDUSTRI I STOCKHOLMSREGIONEN utgår från Näringslivs- och tillväxtstrategin för Stockholmsregionen och ska bidra till visionen om Stockholmsregionen som Europas mest attraktiva storstadsregion. Handlingsplanen avgränsas till delmängden cybersäkerhet av det prioriterade området IKT, tech och digitalisering, vilket är ett av fyra smart specialiseringsområden som har identifierats som strategiskt viktiga för offentliga forsknings- och innovationsinsatser i Stockholmsregionen.[1]

Om cybersäkerhet som konkurrensfördel för Stockholmsregionen

Behovet av cybersäkerhet intensifieras i takt med den accelererande digitaliseringen och allt fler tillämpningar av AI och digitala verktyg inom både offentlig sektor och näringslivet. Under 2021 utsattes 76 procent av Sveriges företagare av IT-relaterad brottslighet åtminstone en gång, med nästan hälften som inte återhämtat sig helt ett år efter attacken[2]. De uppskattade kostnaderna för cybersäkerhetsbrott hos svenska företag uppgick till cirka 30 miljarder kronor år 2021, vilket är en fördubbling jämfört med 2019[3].

Cybersäkerhet är ett gemensamt ansvar som kräver samarbete för att stärka samhällets försvarsförmåga mot cyberangrepp. Samarbetet mellan sektorerna måste klart definiera roller och ansvarsområden för att effektivt kunna bygga en stark och växande cybersäkerhetsindustri i Stockholmsregionen.

I Stockholmsregionen finns framstående forskning och expertis inom cybersäkerhet samt flera snabbväxande företag inom området. Det finns potential för att utveckla ett starkt kluster som sammanför akademisk kunskap med företagande och praktisk expertis. Cybersäkerhet är också avgörande för utvecklingen inom andra specialiserade områden genom att tillhandahålla nödvändig säkerhet och förtroende för teknologier och tjänster.

Det behövs ett samlat grepp om cybersäkerhetssektorns framväxt och samlade behov i Stockholmsregionen. Branschen uttrycker ett behov av nya utbildningsperspektiv och metoder för att täcka det befintliga kompetensgapet. Samarbeten mellan utbildningsinstitutioner, privata företag och offentlig sektor är nödvändiga för att säkerställa att utbildningsprogrammen är relevanta och att de examinerade snabbt kan övergå till arbetslivet. Det behövs neutrala mötesplatser där olika sektorer kan mötas och diskutera cybersäkerhetsrelaterade frågor, och där akademin tillsammans med näringslivet kan interagera kring utmaningar och gemensamma lösningar för en starkare cybersäkerhetsindustri i Stockholmsregionen.

[1] Läs mer om Näringslivs- och tillväxtstrategi för Stockholmsregionen och smart specialisering på sidan 8.
[2] Företagarna "Är det it-säkert?" 2022
[3] Stockholms Handelskammare "Cyberbrott mot svenska företag" 2022

Framtagning

Framtagningen av denna handlingsplan har skett i dialog med Kista Science City, som i sin tur haft dialog och möten med representanter från såväl regionalt som nationellt verksamma aktörer från företag, branschorganisationer, universitet, forskningsinstitut och andra aktuella aktörer. Även relevanta studier och rapporter har använts som underlag i framtagandet av denna handlingsplan.

Genomförande

Handlingsplanerna för smart specialisering genomförs i samverkan mellan Region Stockholm och relevanta aktörer för det aktuella smart specialiseringsområdet. Genomförandet av handlingsplanerna samordnas inom relevanta grupperingar eller nätverk. Vid behov formeras en samordningsgrupp. I enlighet med rekommendationerna från EU-kommissionen ska insatser och utveckling inom de prioriterade områdena för smart specialisering löpande följas upp och utvärderas, vilket Region Stockholm bland annat gör inom ramen för uppföljningen av handlingsplanerna och återrapporteringen till staten. Vid behov justeras handlingsplanernas aktiviteter i samband med uppföljning.

Mål och aktiviteter

För Handlingsplan för en starkare cybersäkerhetsindustri i Stockholmsregionen har tre mål med tillhörande aktiviteter formulerats med utgångspunkt i Näringslivs- och tillväxtstrategins vision och mål för Stockholmsregionens utveckling:

MÅL 1:

Utveckla ett internationellt attraktivt kluster för cybersäkerhet i Stockholmsregionen

Aktiviteter:

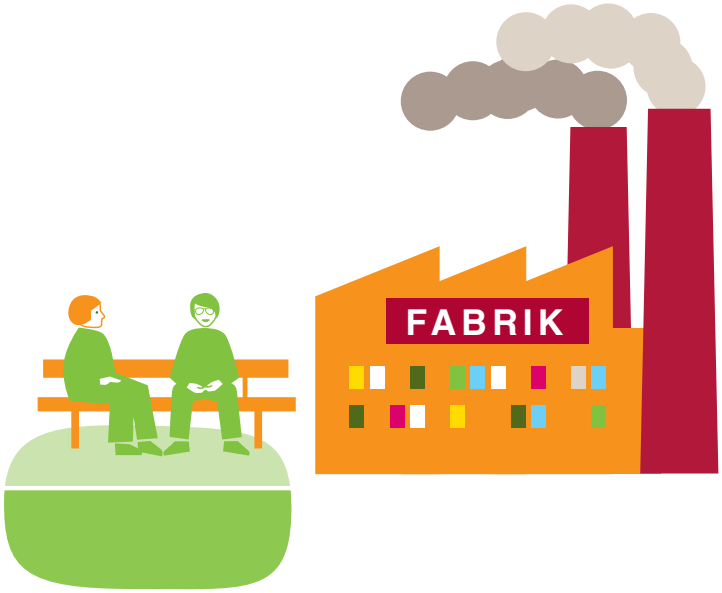
1. Kartläggning och behovsanalys: Genomföra en detaljerad enkät till alla relevanta aktörer (företag, organisationer, akademiska institutioner) för att kartlägga deras verksamhet, behov och utmaningar samt hur dessa kan adresseras genom regionala insatser. Analysera insamlade data för att identifiera trender, kluster och nya möjligheter samt kategorisera typ av cybersäkerhetsbolag.
2. Rapport: Publicera och kommunicera en rapport med resultatet av kartläggningen som tydliggör relevanta områden inom cybersäkerhet, tillväxttrender och Stockholmsregionens internationella styrkeposition inom område. Analysen skall ge en uppfattning om nuvarande förutsättningar för fortsatt tillväxt inom regionen och internationell konkurrenskraft.
3. Identifiering av initiativ och partnerskap: Kartlägg aktuella och framtida initiativ samt möjliga partnerskap som kan främja branschens utveckling, inklusive internationella samarbeten.
4. Klusterbyggande aktiviteter: Organisera och facilitera forum, events och rundabordssamtal som syftar till att stärka nätverk och samverkan inom cybersäkerhetsklustret. Organisera regelbundna workshops och seminarier för att dela kunskap och goda exempel.
5. Utveckling av en attraktiv klusterplattform: Skapa en plattform där företag inom cybersäkerhet kan visa upp sin expertis, främja samarbete och underlätta för internationell exponering och affärsmöjligheter samt samverka med offentlig sektor. Exempelvis genom att införa årliga cybersäkerhetstävlingar där individer och startups kan presentera lösningar på verkliga cybersäkerhetsproblem.
6. Riktade initiativ till små och medelstora företag: Utarbeta riktade initiativ för att hjälpa små och medelstora företag att förbättra sin cybersäkerhetsställning, exempelvis genom cybersäkerhetsrevisioner och utbildningsprogram.
7. Vägledning till offentlig finansiering: Skapa vägledning och stöd för företag och organisationer för att utnyttja offentlig finansiering, särskilt från EU, med syfte att stärka företagens position och utveckling för ökad export och investeringar. (Viktiga nationella partner: Cybernoden och NCC-SE – Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet).
8. Internationaliseringsstöd: Kartlägg befintliga relevanta internationaliseringsstöd och identifiera eventuella behov av nya stöd och rådgivningsprogram till företag som vill expandera internationellt. I samverkan med regionala och nationella aktörer kan eventuella nya stöd utvecklas och tillhandahållas.
9. Framhävande av förebilder och succéhistorier: Aktivt kommunicera framgångshistorier och exempel på förebilder inom cybersäkerhet för att inspirera och visa på möjligheterna inom och/eller utanför Stockholmsregionen.

MÅL 2:

Förmågan att utveckla och attrahera den mest kvalificerade kompetensen inom cybersäkerhet stärks i Stockholmsregionen

Aktiviteter:

1. Kartlägg företagens och aktörernas behov av kompetensförsörjning: Genomföra en enkät till alla relevanta aktörer (företag, organisationer, akademiska institutioner) för att kartlägga deras nuvarande och kommande kompetensbehov.
2. Kartläggning av befintliga utbildningar: Genomföra en detaljerad granskning av nuvarande utbildningsprogram relaterade till cybersäkerhet för att identifiera luckor och möjligheter för förbättringar.
3. Förslag på förbättrat samarbete för ökad kompetens: Utveckla förslag på hur ett närmare samarbete mellan industrin och utbildningssektorn kan se ut, inklusive praktikplatser, gästföreläsningar, och projektarbeten som direkt svarar mot industrins behov.
4. Tillgång till rätt kompetens: Utveckla insatser som stärker små innovativa företag i Stockholmsområdet att hitta personal med rätt kompetens inom cybersäkerhet.
5. Förslag på förbättrat samarbete för rekryteringen av internationella talanger och spetskompetens: Utveckla förslag på hur regionala och nationella aktörer tillsammans kan attrahera fler internationella talanger och spetskompetens inom cybersäkerhet till Sverige och till Stockholmsregionen.
6. Utveckling av nya utbildningsinitiativ: Samarbeta med utbildningsinstitutioner för att skapa nya program och kurser som är direkt anpassade efter branschens krav, inklusive möjligheter för livslångt lärande och fortbildning. (Viktig nationell partner: Cybercampus)
7. Utforska möjligheterna att utveckla nya utbildningsprogram: Utforska möjligheterna för akademin och utbildningsaktörerna att utveckla nya utbildningsprogram inom cybersäkerhet såsom t.ex. yrkesförberedande utbildningar inom cybersäkerhet baserat på industrins behov.
8. Incitament för att stimulera tillväxten av talanger: Kartlägg nuvarande möjligheter och identifiera eventuella nya sätt att stimulera talangtillväxt inom cybersäkerhet inkluderande studenter från grundutbildning upp till forskarnivå.



MÅL 3:

Värdeskapande samarbeten bidrar till nya innovativa lösningar inom cybersäkerhet

Aktiviteter:

1. Skapande av ett Co-lab: Utveckla möjligheter för företag inom cybersäkerhet att samarbeta, utbyta idéer och utveckla nya innovativa lösningar tillsammans med andra intressenter från både offentlig och privat sektor.
2. Co-location möjligheter: Tillhandahålla faciliteter där dessa samverkande parter kan mötas fysiskt för att arbeta intensivt med innovation och produktutveckling.
3. Engagemang av behovsägare: Inbjuda representanter från offentlig och privat sektor samt andra relevanta behovsägare till co-lab för att identifiera utmaningar som kan lösas genom ny teknik och innovation.
4. Innovation genom ökad resiliens inom offentlig sektor: Ta fram gemensamma erbjudanden för offentliga aktörer i Stockholmsregionen för ökad kompetens och resiliens inom cybersäkerhet.
5. Stödinsatser för innovativa företag: Utveckla och genomföra insatser som direkt stöttar företag i utvecklingen av nya produkter och tjänster, inklusive stöd för prototypframtagning och validering av digitala lösningar. Exempelvis inom andra smart specialiseringsområden:
   - Life science, vård och hälsa: utveckla cybersäkerhetslösningar för att skydda känsliga data och system inom hälsosektorn.
   - Industriell omställning genom hållbar produktion; säkerställa cybersäkerhet i omställningen till hållbar produktion och industri 4.0.
   - Klimat- och miljösatsningar för hållbar stadsutveckling; integrera cybersäkerhet i utvecklingen av hållbara stadsprojekt och infrastruktur.
6. Upphandling som innovationskatalysator: Använda offentlig upphandling som ett verktyg för att driva på innovation genom att ställa krav och ge utrymme för innovativa lösningar i upphandlingsprocesser.
7. Internationella samarbeten: Etablera kontakter och inleda samarbete med andra ledande cybersäkerhetsnoder globalt för att utbyta kunskap, erfarenheter och skapa möjligheter för gemensamma innovations- och forskningsprojekt och -samarbeten.

Om smart specialisering i Stockholmsregionen

I juni 2021 antogs Näringslivs- och tillväxtstrategi för Stockholmsregionen som också är regionens Forsknings- och innovationsstrategi för smart specialisering. Näringslivs- och tillväxtstrategin är en konkretisering av Stockholmsregionens utvecklingsstrategi RUFS 2050 och ska bidra till visionen om Stockholmsregionen som Europas mest attraktiva storstadsregion och målen:

- en ledande tillväxt- och kunskapsregion
- en öppen, jämställd, jämlik och inkluderande region

Med utgångspunkt i globala trender, Stockholmregionens styrkor och utmaningar, omfattande analyser och i bred dialog med regionens aktörer genom samtal, workshops och skriftliga inspel har en strategisk inriktning med fyra inriktningsområden identifierats. De fyra strategiska inriktningsområdena att stärka och utveckla är:

- Forskning, innovation och smart specialisering
- Små och medelstora företags konkurrenskraft
- Export, internationalisering och investeringar
- Strategisk kompetensförsörjning

EU-kommissionen lanserade i samband med strukturfondsperioden 2014–2020 begreppet regionala forsknings- och innovationsstrategier för smart specialisering som ett villkor för finansiering av insatser för forskning, innovation och teknisk utveckling ur den regionala utvecklingsfonden (ERUF). Syftet är att identifiera och prioritera ett begränsat antal spetsområden där offentliga medel för forskning och innovation förväntas göra mest nytta och där regionala aktörer har goda förutsättningar att utveckla internationell konkurrenskraft.

Med utgångspunkt i regionala styrkeområden inom näringsliv, forskning och offentlig sektor påbörjades redan 2015 en regional analys- och förankringsprocess genom vilken fyra smart specialiseringsområden har identifierats som strategiskt viktiga för offentliga forsknings- och innovationsinsatser i Stockholmsregionen. Dessa har i flera fall tydlig förankring i olika regionala stadskärnor och deras forsknings- och innovationsmiljöer/kluster. De prioriterade områdena är:

- Life science, vård och hälsa (För detta område finns särskild strategi Life Science-strategi för Stockholmsregionen RS 2019-0751).
- IKT, tech och digitalisering
- Industriell omställning genom hållbar produktion
- Klimat- och miljösatsningar för hållbar stadsutveckling

De områden som har prioriterats för smart specialisering ska stärkas och utvecklas genom insatser från de fyra strategiska inriktningsområdena.

För att nå visionen och målen ovan kan flera aktörer behöva genomföra insatser, såväl inom sina egna organisationer som gemensamt. För att skapa samverkansarenor för samordning av genomförandet tas handlingsplaner fram med ett antal mer konkretiserade mål och aktiviteter.

Region Stockholm