Sex förslag för en stärkt

kompetensförsörjning inom cybersäkerhet

Innehåll

Förslagen i den här rapporten är slutsatserna från en workshop om kompetensförsörjning inom cybersäkerhet som genomfördes under hösten 2023.

Rapporten har tagits fram av: Elin Backström (Universitetskanslersämbetet), Josef Lannemyr (Tillväxtverket), Christer Åhlund (Luleå tekniska universitet) och Callisto Utriainen (Myndigheten för samhällsskydd och beredskap)

Grafisk formgivning av: Antonia Trollmåne, Anna-Carin Pettersson och Mia Hageskog (Arbetsförmedlingen)

Mars 2024

Förord

Denna rapport är resultatet av en konferens som genomfördes 30 november 2023. Då samlades aktörer från myndigheter, utbildningssektorn, bransch och näringsliv för att diskutera och formulera lösningar för att möta den växande efterfrågan på kompetens inom cybersäkerhet.

Konferensen arrangerades av Arbetsförmedlingen, Tillväxtverket och Universitetskanslersämbetet inom ramen för arbetet med en sektorsarena för digital spetskompetens inom myndighetssamverkan för kompetensförsörjning och livslångt lärande. Rapporten har tagits fram av deltagare på konferensen.

Vi tackar alla deltagare för ert engagemang och bidrag i framtagande av dessa förslag.

Myndighetssamverkan för kompetensförsörjning och livslångt lärande
Mars 2024

Vi står bakom rapporten

- Rebecca Tyrstrup, Academic Work
- Per Hammar, Almega Utbildningsföretagen
- Anna Palmgren, Arbetsförmedlingen
- Per Gauffin, Arbetsförmedlingen
- Petra Jansson, Arbetsförmedlingen
- Kurt Tutschku, Blekinge Tekniska Högskola
- Irene Ek, Google Cloud Nordics
- Rose-Mharie Åhlfeldt, Högskolan i Skövde
- Betelhem Teshome, IT-Högskolan
- Emelie Janelöv, IT-Högskolan
- Pontus Johnsson, Kungliga Tekniska högskolan (KTH), Cybercampus Sverige
- Joanna Sjölander, Linköping Science Park
- Mikael Asplund, Linköpings universitet
- Christer Åhlund, Luleå tekniska universitet
- Christine Grosse, Luleå tekniska universitet
- Saguna Saguna, Luleå tekniska universitet
- Sandra Barouta Elvin, Microsoft AB
- Callisto Utriainen, Myndigheten för samhällsskydd och beredskap
- Hanna Lagerquist, Myndigheten för samhällsskydd och beredskap
- Carina Larsson, Myndigheten för yrkeshögskolan
- Christer Bergqvist, Myndigheten för yrkeshögskolan
- Jenny Sörby, Myndigheten för yrkeshögskolan
- Ulrika Hargö, Nackademin
- Kim Elman, RISE
- Shahid Raza, RISE, Cybercampus Sverige, Mälardalens universitet
- SEB
- Petra Klein, Swedbank
- Ronja Ahlberg, Säkerhets- och försvarsföretagen (SOFF)
- Ulf Savbäck, Tillväxtverket
- Marie Kahlroth, Universitetskanslersämbetet

Sammanfattning

Den här rapporten presenterar sex förslag för att stärka kompetensförsörjningen inom cybersäkerhet. Efterfrågan på kompetens inom cybersäkerhet har ökat markant i takt med ett förändrat säkerhetsläge och ett ökat antal cyberangrepp i samhället. För att möta efterfrågan krävs insatser på både kort och lång sikt, riktade mot både den breda allmänheten och yrkesverksamma inom cybersäkerhet.

Förslagen har tagits fram i samverkan mellan myndigheter, utbildningssektor, bransch och näringsliv med utgångspunkt i en gemensam workshop under hösten 2023. Till varje förslag beskriver vi behoven, föreslår lösningar och berättar vad vi behöver göra för att genomföra förslaget. Vi ger också goda exempel och berättar om pågående initiativ som kan relateras till förslaget.

Förslagen både kompletterar och hakar i varandra. Vi presenterar dem i korthet här, utan inbördes ordning:

1. **Kunskapslyft för allmänheten**
   Ett samhällsövergripande kompetenslyft med insatser för att höja den allmänna kunskapen om cybersäkerhet i samhället och på så sätt minska digitala risker.
2. **Baskurser i cybersäkerhet**
   En gemensam plattform med grundläggande kurser inom cybersäkerhet, designade för att kunna ges som fristående kurser eller komplettera ett utbildningsprogram.
3. **Cyberhygien hos nyckelmålgrupper**
   Riktade utbildningsinsatser mot nyckelfunktioner i svenska organisationer för en stärkt säkerhetskultur.
4. **Livslångt lärande för yrkesverksamma**
   Framtagande av kurser för yrkesverksamma, på varierande nivåer och med olika fokus för att anpassas till olika branschers krav, behov och nivå.
5. **Kraftsamling i samverkan**
   En formaliserad samverkan mellan utbildningsanordnare och arbetsmarknadsaktörer, för att utforma relevant utbildningsinnehåll och dimensionera utbildningsplatser.
6. **Bild av kompetensbehovet**
   En förbättrad kartläggning av kompetensbehovet, med fokus på att identifiera centrala yrkesroller och beskriva relevanta förmågor och kompetenser.

I rapporten betonas betydelsen av att olika samhällsaktörer, från både privat och offentlig sektor, tar gemensamt ansvar för att genomföra förslagen. Även regeringen spelar en avgörande roll i att skapa förutsättningar, inte minst finansiellt, och fördela samordningsansvar till lämpliga myndigheter när det krävs.

Vi hoppas att rapporten kan fungera som inspiration till kommande strategier och beslut samt underlätta samarbetet mellan de aktörer som kan bidra till att förverkliga förslagen.

01

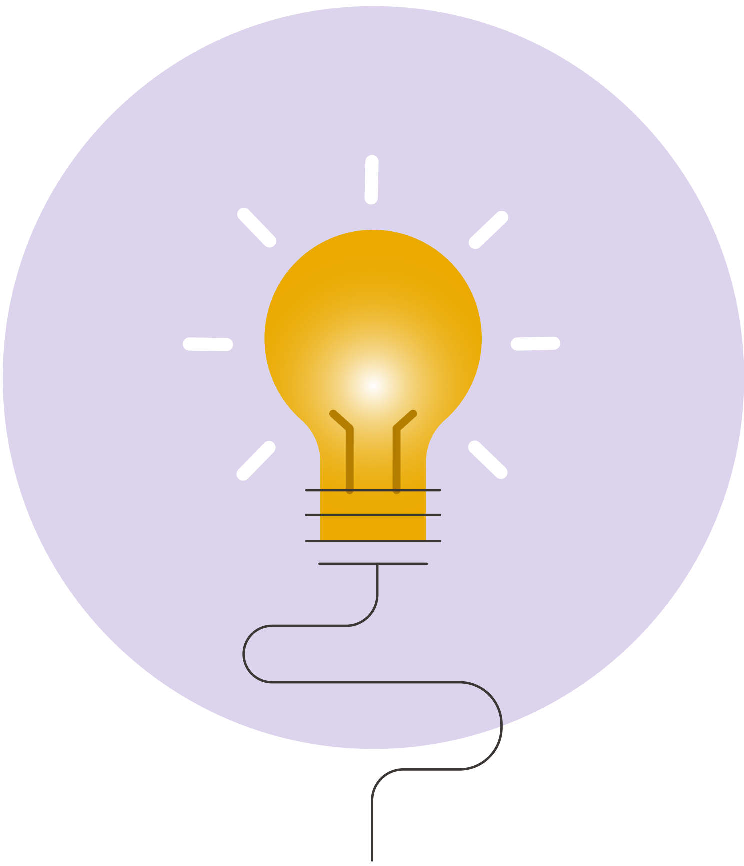
BAKGRUND OCH INSIKTER

Insatser behövs för att möta kompetensbehovet inom cybersäkerhet

I takt med digitaliseringens framsteg och ett förändrat säkerhetsläge har efterfrågan på kompetens inom cybersäkerhet ökat markant. Efterfrågan är ett globalt fenomen som drivs av behovet av att säkra data, information och flöden i en digital infrastruktur, samt upprätthålla ett försvar mot de cyberattacker som hotar dem.[1] För att möta detta kompetensbehov och stärka samhällets resiliens behövs insatser på både kort och lång sikt.

I den här rapporten presenteras sex förslag för att stärka kompetensförsörjningen inom cybersäkerhet i Sverige. Förslagen har tagits fram i samverkan mellan myndigheter, utbildningssektor, bransch och näringsliv med utgångspunkt i en gemensam workshop hösten 2023. Workshopen arrangerades inom ramen för arbetet med en sektorsarena för digital spetskompetens inom Myndighetssamverkan för kompetensförsörjning och livslångt lärande.[2]

Syftet med rapporten är att öka medvetenheten om kompetensbehoven inom cybersäkerhet och visa på möjliga lösningar. Rapporten är tänkt att fungera som inspiration till kommande strategier och beslut samt underlätta samarbetet mellan de aktörer som kan bidra till att förverkliga förslagen. Förslagen riktar sig till regeringen, myndigheter, utbildningsanordnare samt bransch- och näringslivsaktörer.

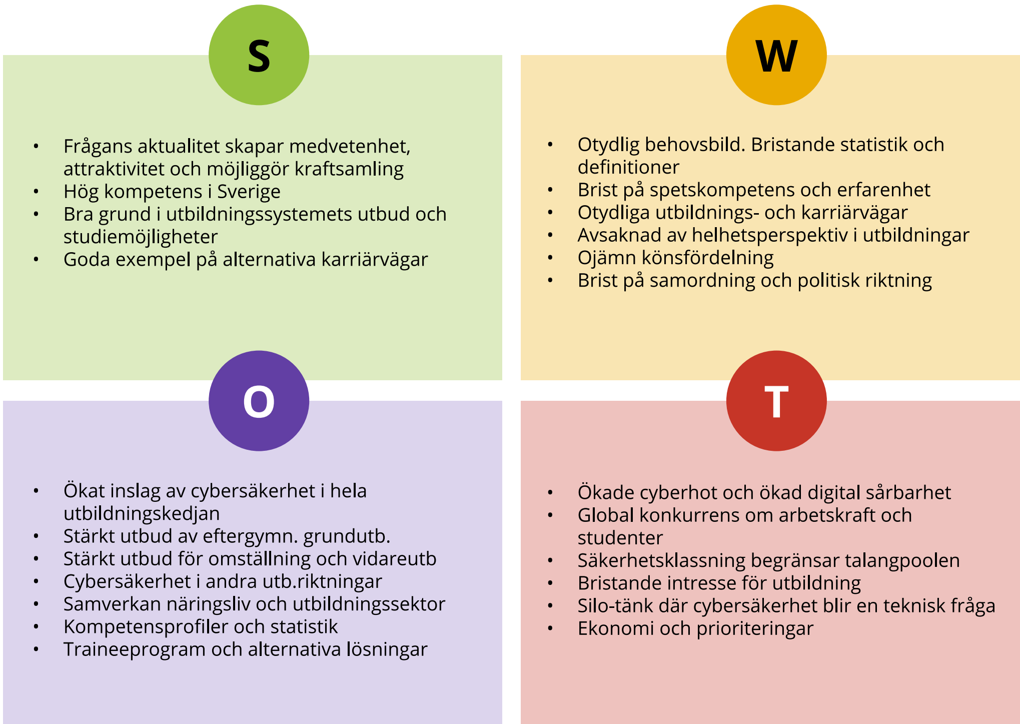


1 IVA. *Cybersäkerhet för ökad konkurrenskraft*. Kungl. Ingenjörsvetenskapsakademin, 2022; MSB. *Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället*. Myndigheten för samhällsskydd och beredskap, 2021.
2 Arbetsförmedlingen, Myndigheten för yrkeshögskolan, Skolverket, Svenska ESF-rådet, Tillväxtverket, Universitetskanslersämbetet och Universitets- och högskolerådet har fått i uppdrag att samverka för att bidra till en väl fungerande kompetensförsörjning. Även Folkbildningsrådet och Vinnova ingår i samarbetet.

Kompetensförsörjning inom cybersäkerhet är en växande utmaning

Det här avsnittet ger en bild av nuläget och de förutsättningar som finns för att möta den växande efterfrågan på cybersäkerhetskompetens i Sverige. Figur 1 visar nuläget i form av en analys av styrkor, svagheter, möjligheter och hot (SWOT-analys), som togs fram i samband med workshopen 2023. Läs mer om SWOT-analysen i bilaga 1.

Figur 1. SWOT-analys av de styrkor (S), svagheter (W), möjligheter (O) och hot (T) som finns kopplat till kompetensförsörjning inom cybersäkerhet.



Efterfrågan på cybersäkerhetskompetens ökar både i Sverige och internationellt

Både internationella och nationella rapporter pekar på en utbredd kompetensbrist inom cybersäkerhet. Enligt ISC2:s årliga studie Cybersecurity Workforce Study från 2023 består arbetskraften inom cybersäkerhet i hela världen av 5,5 miljoner personer, där arbetstillfällena ökar varje år med 8,7 procent. För Europa handlar det om 1,3 miljoner personer, där arbetstillfällena varje år ökar med 7,3 procent. Men samtidigt som arbetskraften växer ökar också kompetensgapet. ISC2 bedömer att det globalt saknas nära 4 miljoner personer med cybersäkerhetskompetens, varav ungefär 350 000 i Europa. Efterfrågan på kompetens förväntas växa snabbare än antalet yrkesverksamma inom området. Det gör bristen på kompetens, liksom den globala konkurrensen om den, till en fortsatt utmaning.[3]

I Sverige finns inga exakta beräkningar av hur många yrkesverksamma som behövs inom cybersäkerhetsområdet. Bedömningarna försvåras bland annat av att cybersäkerhetskompetensen döljer sig bakom olika roller och titlar.

3 ISC2. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. ISC2 Cybersecurity Workforce Study, 2023.

Kompetensen som efterfrågas är ofta tvärfunktionell och multidisciplinär i sin karaktär, och behoven varierar beroende på bransch, sektor och legala krav. Det gör det svårt att ta fram statistik om hur många som jobbar inom området och hur många som behövs för att fylla kompetensbehovet framöver.[4] Att det saknas en samlad bild av kompetensbehovet i Sverige försvårar planeringen av kompetensförsörjningsinsatser. Till exempel blir det svårt att matcha utbildningsutbudet mot arbetsmarknadens behov.[5]

Flera svenska undersökningar visar samtidigt att efterfrågan på kompetens växer i Sverige.[6] TechSveriges senaste rapport om kompetensbehoven inom techbranschen beskriver att informations- och cybersäkerhetskompetens är en av de trender som förväntas påverka arbetsgivares kompetensbehov starkast framöver.[7] Det resultatet ligger i linje med Arbetsförmedlingens långsiktiga yrkesområdesprognos inom data och it, där det konstateras att antal platsannonser för it-säkerhetsspecialister har ökat med drygt 270 procent från 2016 till 2021. Det är den största procentuella utvecklingen inom hela yrkesområdet data och it.[8]

Både specialiserad och allmän kompetens behövs framöver

Behovet av kompetens inom cybersäkerhet behöver förstås ur ett brett perspektiv, där efterfrågan på både allmän och specialiserad kompetens måste mötas. Till exempel finns behov av

- en allmän kunskapshöjning i samhället, där gemene man får högre kompetens i sin personliga digitala hantering och därmed kan minska risken för kriminella handlingar som stöld av pengar och utpressningsattacker
- en stärkt kompetens hos medarbetare som inte arbetar med cybersäkerhet, men som genom sin yrkesutövning behöver ha tillräcklig kompetens för att minska organisationens digitala risker
- en kunskapshöjning inom organisationers ledningsnivåer, där cybersäkerhet hanteras som en strategisk fråga av betydelse för hela verksamheten
- en ökad kompetens i *security by design*, där medarbetare på it-företag får kunskap i att bygga in säkerhet i systemen från grunden och säkerställa cybersäkerheten både när man utvecklar och använder produkter och tjänster
- en stärkt specialistkompetens för systemdrift, underhåll och hantering av faktiska cyberattacker, där organisationer får kapacitet att kontinuerligt övervaka och snabbt reagera på cyberhot.[9]

Flera undersökningar pekar på att arbetsgivare framför allt vill rekrytera personer med lång erfarenhet och med specialistkompetens inom cybersäkerhet.[10] Det kan skapa utmaningar för juniora och nyexaminerade personer, vars kompetens ännu inte matchar efterfrågan på arbetsmarknaden. Därmed kan insatser som traineeprogram vara viktiga för att sänka trösklarna för ett inträde i branschen.

4 MSB, *Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället*.
5 TechSverige. *Techbranschens förslag för att möta cyberhoten*. TechSverige, 2023.
6 Se till exempel IVA, *Cybersäkerhet för ökad konkurrenskraft; MSB, Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället; SOFF. Vilka kompetenser och färdigheter söker Sveriges säkerhets- och försvarsföretag? En rapport om vilka cyberkompetenser SOFF:s medlemsföretag inom cyberområdet efterfrågar. Säkerhets- och försvarsföretagen, 2022; Svenskt Näringsliv. Företagen och IT-säkerheten – hotbilder, motåtgärder och behov*. Svenskt Näringsliv, 2021.
7 TechSverige. *Kompetensbehoven inom tech*. TechSverige, 2024.
8 Arbetsförmedlingen. *Långsiktig yrkesområdesanalys. Data/it*. Arbetsförmedlingen, 2023.
9 PaloAlto. UNIT 42, Attack Surface Threat Report. PaloAlto 2023; MSB, *Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället*.
10 TechSverige. *Kompetensbehoven inom tech; SOFF, Vilka kompetenser och färdigheter söker Sveriges säkerhets- och försvarsföretag? En rapport om vilka cyberkompetenser SOFF:s medlemsföretag inom cyberområdet efterfrågar; MSB, Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället*.

Cybersäkerhet är en angelägenhet för hela samhället

Cybersäkerhet är en fråga som berör hela samhället. Det är inte längre något som kan hanteras enskilt på it-avdelningar, utan något som berör hela organisationer och privatpersoner. Olika yrkesgrupper, till exempel inom hälso- och sjukvård, utbildning, journalistik, politik och juridik, behöver alla kunna relatera till cybersäkerhet och utveckla den kunskap som är nödvändig för att bidra till samhällets digitala säkerhet. Kompetens behövs i hela spannet, från de som upphandlar eller skriver styrdokument till de som hanterar brandväggar och funktioner för intrångsdetektering.

Nya lagar och ramverk driver också på behovet av nationell kompetensförsörjning inom cybersäkerhet. Exempelvis innebär de ny EU-direktiven NIS2-direktivet, CER-direktivet och förslaget om EU:s Cyber Resilience Act en hög gemensam nivå på säkerhet i nätverk och informationssystem.[11] Det ställer nya krav på organisationer att öka sin kunskap och beredskap.

Arbetet med cybersäkerhet måste även gå i takt med samhällets övergripande digitalisering. Säkerhet börjar i den drift och it-användning som utförs varje dag. Men många tror att även digitala utvecklingstrender som artificiell intelligens (AI) kommer att påverka cybersäkerheten, på både gott och ont. Genom AI kan vi öka förmågan att identifiera cyberhot, samtidigt som cyberattacker och illasinnad påverkan kommer att bli mer komplexa.[12]

Sverige har goda förutsättningar att möta kompetensbehovet

Sverige har i dag en stark position inom digitalisering, både inom näringslivet och offentlig sektor. I internationella jämförelser av digitalisering ligger Sverige i regel i topp. Sverige ligger på fjärde plats i EU-kommissionens Digital Economy and Society Index (DESI), där Europas länder rankas utifrån ett antal områden som är viktiga för digitaliseringen. I jämförelsen sticker Sverige ut med en hög andel it-specialister bland de sysselsatta, vilket är en viktig bas för försörjningen av it-säkerhetskompetens.[13]

Sverige har också ett brett utbud av utbildningar inom cybersäkerhetsområdet, som arrangeras av bland annat universitet och högskolor, yrkeshögskolor och kommersiella aktörer.[14] Utbudet skapar förutsättningar att bygga vidare på och skala upp redan befintliga goda exempel. I och med regeringens satsning på det nyinrättande Cybercampus Sverige finns också möjligheter att forma en utbildnings- och forskningsmiljö med en större kritisk massa av spetsforskning och spetsutbildning inom cybersäkerhet än vad som existerar i Sverige i dag. Cybercampus Sverige är en nationell satsning för att stärka kompetensförsörjningen och forskningen inom cybersäkerhet. Det kommer att vara ett samarbete mellan flera universitet, forskningsinstitut, myndigheter och företag över hela Sverige. Kungl. Tekniska högskolan (KTH) har tilldelats medel för att bygga upp utbildning och forskning inom ramen för satsningen. [15]

---

11 European Commission. *Cyber Resilience Act*, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.; European Commission. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. [Hämtade 2024-02-15]

12 Ansari m.fl. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review (September 2022). *International Journal of Advanced Research in Computer and Communication Engineering* 2022.

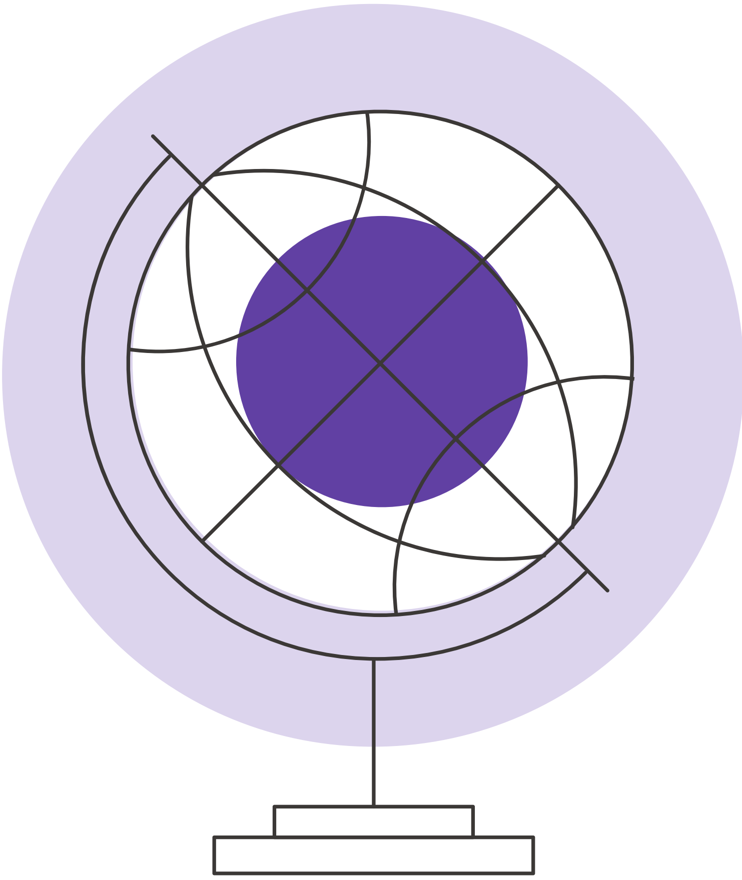
13 DESI. *Index för digital ekonomi och digitalt samhälle (Desi) 2022 Sverige*. Europeiska kommissionen, 2022.

14 Ahmed & Mattsson. *Nationell kompetensförsörjning inom it-, informations- och cybersäkerhetsområdet*. KnowIT, 2023

15 Regeringskansliet. *Regeringen satsar på svenskt cybercampus vid KTH*. https://www.regeringen.se/pressmeddelanden/2023/09/regeringen-satsar-pa-svenskt-cybercampus-vid-kth/. [Hämtad 2024-01-25]

Även om förutsättningarna för att bygga upp cybersäkerhetskompetens i Sverige i grunden är goda, krävs det ytterligare åtgärder för att öka attraktiviteten för utbildningarna och höja medvetenheten om cybersäkerhet. Det gäller särskilt bland allmänheten, som behöver stärka sin medvetenhet om cybersäkerhet redan i ung ålder och sedan få möjlighet att utveckla den kontinuerligt.[16]

EU-kommissionen konstaterar i sin DESI-rapport att ”framstegen [i Sverige] inte är lika snabba som tidigare” på digitaliseringsområdet.[17] Bristen på relevant kompetens pekas ut som ett primärt hinder och bristen på digital spetskompetens är en flaskhals för innovation och tillväxt i Sverige.[18] Sammanfattningsvis krävs breda satsningar för att öka kompetensen i cybersäkerhet i Sverige samt hantera de utmaningar och hot som uppstår i en alltmer digitaliserad värld.



16 ENISA. *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*. ENISA, 2021; Ricci m.fl. Understanding Cybersecurity Education Gaps in Europe. *IEEE Transactions on Education*, 2024, 1–12.
17 DESI. *Index för digital ekonomi och digitalt samhälle (Desi) 2022 Sverige*.
18 OECD. *OECD Reviews of Digital Transformation: Going Digital in Sweden*. OECD, 2018.

02

FÖRSLAGEN

Sex förslag för en stärkt kompetensförsörjning inom cybersäkerhet

I det här avsnittet presenterar vi sex förslag för att stärka Sveriges kompetensförsörjning inom cybersäkerhet. Förslagen är inspirerade av de idéer som myndigheter, bransch, näringsliv och utbildningssektor diskuterade under en workshop hösten 2023.

Under workshopen fick deltagarna diskutera och utveckla idéer för att stärka Sveriges kompetensförsörjning inom cybersäkerhet. Deltagarna fick ge synpunkter på varandras idéer i olika steg och slutligen presentera ett prioriterat förslag. Vi har därefter bearbetat och utvecklat förslagen utifrån en övergripande omvärldsanalys samt en inventering av pågående initiativ och goda exempel. Vi presenterar förslagen i rapporten utan inbördes ordning.

1. **Kunskapslyft för allmänheten**
   Ett samhällsövergripande kompetenslyft med insatser för att höja den allmänna kunskapen om cybersäkerhet i samhället och på så sätt minska digitala risker.
2. **Baskurser i cybersäkerhet**
   En gemensam plattform med grundläggande kurser inom cybersäkerhet, designade för att kunna ges som fristående kurser eller komplettera ett utbildningsprogram.
3. **Cyberhygien hos nyckelmålgrupper**
   Riktade utbildningsinsatser mot nyckelfunktioner i svenska organisationer för en stärkt säkerhetskultur.
4. **Livslångt lärande för yrkesverksamma**
   Framtagande av kurser för yrkesverksamma, på varierande nivåer och med olika fokus för att anpassas till olika branschers krav, behov och nivå.
5. **Kraftsamling i samverkan**
   En formaliserad samverkan mellan utbildningsanordnare och arbetsmarknadsaktörer, för att utforma relevant utbildningsinnehåll och dimensionera utbildningsplatser.
6. **Bild av kompetensbehovet**
   En förbättrad kartläggning av kompetensbehovet, med fokus på att identifiera centrala yrkesroller och beskriva relevanta förmågor och kompetenser.

De olika förslagen går i varandra. I ett kunskapslyft för allmänheten kan till exempel baskurser i cybersäkerhet vara en viktig komponent. Likaså kan en kraftsamling i samverkan vara viktigt för att gemensamt skapa samsyn och ge en bild av kompetensbehovet. Förslagen kan också haka i pågående initiativ, och förstärka satsningar som redan är i gång. Ett sådant exempel är det nyetablerade Cybercampus Sverige.[19]

19 Läs mer om Cybercampus Sverige på https://www.cybercampus.se/ [Hämtad 2024-01-25]

1. Kunskapslyft för allmänheten

Behovet

Samhällets försvar mot cyberhot och cyberattacker är beroende av att Sveriges befolkning har en allmän cybersäkerhetkompetens. I dagsläget bedömer vi att baskunskaperna är låga. Med en ständigt accelererande teknisk utveckling och mer sofistikerade cyberattacker ökar behovet av att höja allmänhetens kunskap om cybersäkerhet. Det gäller inte minst bland barn och ungdomar, som är den framtida arbetskraften. Med en höjd kompetens hos allmänheten kan de digitala riskerna minska, vilket i sin tur minskar behovet av cybersäkerhetsspecialister. Med en ökad medvetenhet finns även potential att skapa ett ökat intresse för att studera och arbeta inom branschen.

Vår lösning

Vi behöver ett samhällsövergripande kompetenslyft för digital säkerhet, där aktörer på olika nivåer bidrar med insatser riktade till olika målgrupper i samhället. Förslaget är att under åtminstone tre år arbeta med till exempel allmänna informationskampanjer, temaveckor i skolor, lärande spelaktiviteter (*gamification*), studiecirklar för privatpersoner, kompetenshöjande seminarier och coachning för företag, hackatons och cyberkrisövningar. Med en bredd av insatser kan vi nå hela befolkningen på ett anpassat vis. Cybersäkerhet kan då bli ett mer naturligt inslag i alltifrån förskola till folkbildning, som kan skapa engagemang och gemensamt ansvarstagande.

Vad behöver vi göra?

Kunskapslyftet kräver insatser från olika sektorer och aktörer. Förutom de traditionella utbildningsaktörerna bör andra relevanta myndigheter, det privata näringslivet och den ideella sektorn, agera för att bidra med insatser, sprida sin kunskap och ta fram goda exempel.

För att öka genomslaget av kunskapslyftet bör en aktör utses för att samordna arbetet. Vi behöver undersöka om aktören kan få särskilda medel som ska distribueras till utförare. Andra aktörer får i sin tur ge förslag på insatser och söka finansiering från samordnaren.

Goda exempel och pågående insatser

Under 1990-talet genomfördes flera stora satsningar för att höja allmänhetens digitala kompetens. Koncept som ”datorkörkort” introducerades, där utbildningar skulle säkerställa att befolkningen fick en grundläggande kunskap i datorhantering. ”Hem-PC-reformen” möjliggjorde för många att köpa en dator för privat bruk, vilket höjde kompetensen. Det visar på potentialen i att underlätta för befolkningen att höja sin digitala kompetens genom breda insatser i samverkan.

I dag finns många exempel på kompetenshöjande satsningar. Det finns flera verktyg för *gamification* som kan användas i utbildningssyfte.[20] Det finns också många utbildningar riktade till företag och yrkesaktiva (se beskrivningar under förslag 3 och 4). Informationskampanjer har riktats till allmänheten, som kampanjen ”Bli inte lurad” från Myndigheten för psykologiskt försvar.[21] Varje år genomför också Polisen och MSB i samarbete kampanjen “Tänk säkert” som riktar sig till privatpersoner för att höja den allmänna medvetenheten om och kompetensen inom cybersäkerhet.[22] Även Internetstiftelsen har publicerat flera guider i säkerhet för privatpersoner.[23]

20 Se till exempel Hackschield https://se.joinhackshield.com/sv och Minecraft Education https://education.minecraft.net/en-us/discover/cyber-and-digital-safety. [Hämtade 2024-02-01]
21 Myndigheten för psykologiskt försvar. *Bli inte lurad*. https://www.bliintelurad.se/. [Hämtad 2024-02-01]
22 MSB. *Tänk säkert*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikatio-ner/informationssakerhetsmanaden/tank-sakert/. [Hämtad 2024-02-01]
23 Internetstiftelsen. *Kunskap*. https://internetstiftelsen.se/kunskap/. [Hämtad 2024-02-01]

2. Baskurser i cybersäkerhet

Behovet

För att möjliggöra ett kunskapslyft inom cybersäkerhet (se förslag 1) behövs ett utbud av flexibla baskurser, som ger en grundläggande kompetens inom cybersäkerhet. Det behöver även finnas kurser som når både studenter och yrkesverksamma som *inte* studerar eller arbetar inom data, it eller cybersäkerhet. Till exempel behöver cybersäkerhet enklare kunna bli ett komplement till utbildning inom bland annat juridik, ekonomi, hälso- och sjukvård och ledarskap. Utöver att baskurser stärker kompetensbasen kan det inspirera till vidare studier eller ett arbete inom cybersäkerhet.

Vår lösning

Vi behöver ta fram kortare grundläggande kurser inom cybersäkerhet, som designas för att kunna ges som fristående kurser eller komplettera ett utbildningsprogram. Kurserna kan vara av olika omfattning, från mindre till större kurser. Kurserna kan ges av flera utbildningsanordnare, på olika nivåer, men också erbjudas som öppna, nätbaserade kurser (så kallade MOOC:ar).[24] På så vis kan basutbildning både bli tillgänglig för allmänheten och samtidigt bli ett verktyg för högskolan och yrkeshögskolan att skapa ett flexibelt kursutbud där cybersäkerhet når fler studentgrupper. Kurserna behöver baseras på en kontinuerlig omvärldsbevakning för att hållas aktuella och relevanta.

För att tillgängliggöra utbudet bör baskurserna samlas på en gemensam plattform. En sådan plattform bör tas fram i samverkan mellan olika utbildningsanordnare. Det blir lättare för allmänheten att hitta lämpliga kurser när de får en samlad bild av utbildningsutbudet, samtidigt som utbildningsanordnarna lättare kan identifiera eventuella luckor i utbudet.

Vad behöver vi göra?

För att genomföra baskurserna krävs engagemang och insatser från olika utbildningsanordnare som kan erbjuda kurserna, bland annat universitet, högskolor och yrkeshögskolor. Även ideella organisationer och privata utbildningsanordnare skulle kunna vara lämpliga utförare.

För att stärka förutsättningar att ta fram öppna, nätbaserade utbildningar, bör man även överväga att ge särskilda finansieringsmöjligheter under en expansionsfas. Under en sådan fas kan man rikta medel till lärosäten och andra utbildningsanordnare för att utveckla kursutbudet.

Cybercampus Sverige är en aktör som skulle kunna bidra till samordning i en fråga av det här slaget. Vid Cybercampus pågår även ett arbete med att utveckla kurser, där ett förslag berör just grundläggande kurser för allmänheten.[25] Därmed finns möjliga synergier med det här förslaget.

Goda exempel och pågående insatser

I dag finns ett relativt stort kursutbud hos svenska utbildningsanordnare, med kurser på grundläggande nivå. Dessa kurser skulle kunna lyftas in och marknadsföras i en gemensam portal. Tidigare satsningar som *AI Competence for Sweden*[26] eller *Öppet för klimatet*[27] kan bli förebilder för hur öppna nätbaserade kurser kan tas fram och presenteras. Satsningarna är också goda exempel på hur ett kursutbud kan samlas och bli tillgängligt via en gemensam digital plattform.

24 En MOOC (Massive Open Online Course) innebär att kursen erbjuds digitalt via en online-plattform, har obegränsat antal platser, är gratis och kan sökas av vem som helst.
25 Gunnar Karlsson, Paola Lundén, *Agile Education Imagined: A report from the Cybercampus workshop on Agile Education*, KTH TRITA-EECS-RP 2023:1, January 2023.
26 AI Competence for Sweden, https://ai-competence.se/. [Hämtad 2024-02-05]
27 Learning 4 professionals, *Öppet för klimatet*, https://learning4professionals.greentown.se/oppet-for-klimatet/. [Hämtad 2024-02-05]

3. Cyberhygien hos nyckelmålgrupper

Behovet

Svenska organisationer behöver höja sitt säkerhetsmedvetande och stärka sin säkerhetskultur. Det gäller alltifrån statliga myndigheter till kommuner, regioner, privata företag och ideella organisationer. För att åstadkomma det behöver nyckelfunktioner i organisationer grundläggande förståelse för cybersäkerhet. Det kan exempelvis handla om politiker, ledare, förvaltningschefer, skolchefer, utbildare och upphandlare. Dessa målgrupper behöver öka sin kompetens för att aktivt kunna arbeta med cybersäkerhet och systematiskt informationssäkerhetsarbete inom sina ansvarsområden. Det gynnar både deras egna organisationer och samhället som helhet genom en förbättrad och hållbar cyberhygien, samtidigt som kompetensnivån i samhället höjs.

Vår lösning

Ett första steg är att genomföra en kartläggning för att identifiera prioriterade målgrupper och deras behov. Kartläggningen gör det lättare att utforma utbildningsinsatser riktade mot specifika behov hos respektive målgrupp. Utbildningsinsatserna kan delvis vara baskurser i cybersäkerhet för olika sektorer, som erbjuds på en gemensam digital plattform (se förslag 2 på sidan 13). Det kan även vara mer nätverksskapande insatser, som studiecirklar om systematiskt informationssäkerhetsarbete.

En utbildningsinsats skapar ringar på vattnet, där utbildade individer inom varje målgrupp agerar som ambassadörer för området och sprider sin kunskap vidare. Det skapar en ökad medvetenhet och engagemang i frågan om cybersäkerhet och lägger grunden för att skapa bättre policyer och bestämmelser. När deltagarna i utbildningarna sedan skapar nätverk, blir det lättare för dem att byta erfarenheter och samarbeta.

Vad behöver vi göra?

En lämplig aktör bör få i uppdrag att identifiera prioriterade målgrupper och deras behov samt undersöka hur de befintliga utbildningsmöjligheterna möter de behoven. Aktören bör ge förslag på kompletterande utbildningsmöjligheter samt hur de kan finansieras, exempelvis via EU:s regionala fonder. Viktiga för själva utförandet av kompetensinsatserna blir till exempel utbildningsanordnare, myndigheter, företagsnätverk och branschorganisationer.

Goda exempel och pågående insatser

Inom Cybercampus håller man på att ta fram en utbildningskatalog. Det finns förslag på ett brett utbud av kurser och utbildningsformer som kan anpassas efter olika behov hos olika grupper.[28]

Goda exempel på riktade kompetensinsatser finns även bland olika *science parks.* Där kan man etablera regionala samverkansplattformar för att koordinera och underlätta samarbetet om digital säkerhet mellan näringsliv, akademi, myndigheter och institut.

Flera myndigheter har eller har haft uppdrag inom det här området. Exempelvis erbjuder MSB utbildningar riktade mot chefer inom cybersäkerhet, CISO:er (Chief Information Security Officers).[29] Tillväxtverket har tidigare haft uppdrag att höja kompetensen om digitalisering i små och medelstora företags styrelser, för att öka medvetenheten om behovet av informationssäkerhet.[30]

---

28 Karlsson & Lundén, *Agile Education Imagined: A report from the Cybercampus workshop on Agile Education*.
29 MSB. *Kurser i informationssäkerhet*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/kurser-i-informationssakerhet/. [Hämtad 2024-02-15]
30 Tillväxtverket fick 2018 regeringsuppdraget Höjd digital kompetens i småföretags ledningar och styrelser. Se rapporten *Säker digitalisering i små och medelstora företag Kartläggning av behov och initiativ på marknaden*, Tillväxtverket, 2021.

4. Livslångt lärande för yrkesverksamma

Behovet

De som redan arbetar inom cybersäkerhet behöver få möjlighet till kontinuerlig kompetensutveckling, för att hålla sig uppdaterade med utvecklingen inom cybersäkerhetsområdet. Även de som är yrkesverksamma inom närliggande områden behöver få möjlighet att komplettera eller bygga på sin kompetens, så att tillgången på arbetskraft ökar. För att det här ska bli möjligt behövs ett större och mer flexibelt utbud av kurser för yrkesverksamma.

Vår lösning

Vi behöver ta fram fler kurser för yrkesverksamma, både grundläggande och specialinriktade på olika branscher. Det innebär att kursernas innehåll kan variera stort. De grundläggande kurserna kan vara basutbildningar för yrkesverksamma som saknar tekniska förkunskaper, till exempel enligt förslag 2 (se sida 13). De specialinriktade kurserna kan vara vidareutbildning för yrkesverksamma inom it som vill bygga på med specialistkunskaper inom cybersäkerhet.

Utbildningarna bör vara flexibla till sin form och komma i olika format, till exempel klassrumsbaserad undervisning, onlinekurser och workshoppar. Ett viktigt moment är att integrera praktiska övningar och scenariobaserad träning, för att öka tillämpningen av teoretiska kunskaper och säkerställa fortbildningens relevans. Därför behöver man rekrytera kvalificerade yrkesverksamma experter inom cybersäkerhet som utbildare och handledare.

Vad behöver vi göra?

Satsningen kan delvis betraktas som en del av högskolans och yrkeshögskolans anpassning för livslångt lärande och omställning. Men under en inledande expansionsfas bedömer vi att det behövs särskilda möjligheter att finansiera insatserna, där lärosäten och andra utbildningsanordnare får medel för att utveckla ett kursutbud för yrkesverksamma. Även privata utbildningsföretag spelar en viktig roll för att ta fram och erbjuda ett utbildningsutbud för livslångt lärande.

Goda exempel och pågående insatser

I dag finns flera exempel på branschanpassade kurser för yrkesverksamma vid till exempel högskolan och yrkeshögskolan.[31] Även här finns ett pågående utvecklingsarbete vid Cybercampus Sverige, med förslag på utbildningsinsatser riktade mot yrkesverksamma.[32] Likaså kan inspiration hämtas från *LUPP-projektet – samverkan om livslångt lärande och uppdragsutbildning* och programmet *Expertkompetens*, där lärosäten får möjlighet att tillsammans med företag utveckla sin förmåga att möta näringslivets behov av kompetensutveckling för yrkesverksamma.[33]

I budgetpropositionen för 2024 föreslog regeringen en satsning på korta kurser för yrkesverksamma, för att stärka kompetensförsörjningen för den gröna omställningen. Ett antal lärosäten kommer att få medel för organisering och utveckling.[34] Liknande finansieringsupplägg skulle kunna vara aktuellt för att expandera utbudet även inom cybersäkerhetsområdet.

31 Se till exempel Högskolan Väst. *Introduktion till industriell cybersäkerhet*, https://www.hv.se/utbildning/kurs/introduktion-till-industriell-cybersakerhet-deltid-distans-iic600/ eller IT-högskolan. *IT-säkerhet, YH-kurs*. https://www.iths.se/utbildningar/it-sakerhet/. [Hämtade 2024-02-14]
32 Karlsson & Lundén, *Agile Education Imagined: A report from the Cybercampus workshop on Agile Education*.
33 Vinnova. *Samverkan för livslångt lärande – uppdragsutbildning*, https://www.vinnova.se/p/samverkan-for-livslangt-larande---uppdragsutbildning/; KK-stiftelsen. *Expertkompetens*, https://www.kks.se/program/expertkompetens/. [Hämtade 2024-02-14]
34 Regeringskansliet, Korta kurser för yrkesverksamma som vill vidareutbilda sig eller ställa om i yrkeslivet ska stärka kompetensförsörjningen för den gröna omställningen. [Hämtad 2024-02-22]

5. Kraftsamling i samverkan

Behovet

Företag, myndigheter och utbildningsanordnare har ett uttalat behov av en fördjupad och mer formaliserad samverkan om kompetensförsörjning inom cybersäkerhet. För att effektivt hantera utmaningar med till exempel utbildningars dimensionering och innehåll, behöver utbildningsanordnare och arbetsmarknadsaktörer få möjlighet till dialog där de kan skapa samsyn. Genom att förbättra samverkan mellan dessa parter ökar möjligheterna att långsiktigt stärka främjandet av cybersäkerhetsspetskompetens och säkerställa att utbildningsutbudet återspeglar den faktiska efterfrågan på kompetens.

Vår lösning

För att underlätta samverkan om kompetensförsörjning behöver en aktör få ett tydligt uppdrag att koordinera och främja samverkan mellan utbildningsanordnare, arbetsmarknadsaktörer, myndigheter och andra relevanta parter.

Huvuduppgiften för samverkanskonstellationen är att bedöma behovet av kompetensförsörjning för cybersäkerhet och relatera behoven till relevanta utbildningsmöjligheter. Det är viktigt att även inkludera diskussioner om sektorns förmåga till mångfald och inkludering samt forskning och innovation i samtalet. Likaså behöver diskussionerna ta hänsyn till hur nya regulatoriska krav påverkar kompetensbehovet. Genom att bredda diskussionen till de områdena kan samarbetet säkerställa mer övergripande och hållbara strategier, för att stärka samverkansparterna och möta deras framväxande behov.

Vad behöver vi göra?

En lämplig aktör bör få i uppdrag att samordna arbetet med kompetensförsörjning inom cybersäkerhet. För att få kraft i samverkan behöver relevanta aktörer från bland annat utbildningssektorn, myndigheter, branschorganisationer och det privata näringslivet delta aktivt i samarbetet.

Goda exempel och pågående insatser

Det finns flera olika exempel på hur samverkan kan organiseras. På regional nivå finns bland annat Göteborgsregionens kompetensråd, där samverkan sker både strategiskt och branschspecifikt. Branschföreträdare, företag, fackförbund, utbildningsanordnare och omställningsorganisationer samarbetar, för att stärka matchningen på arbetsmarknaden. Det sker genom omvärldsbevakning, erfarenhetsutbyte, gemensamma utvecklingsinsatser och aktiviteter.[35] På nationell nivå finns till exempel Nationella vårdkompetensrådet, som är ett rådgivande organ som ska bidra till en god planering av vårdens kompetensförsörjning genom att bland annat bedöma kompetensbehoven.[36]

Inom cybersäkerhet finns befintliga nätverk som kan bidra till att samla relevanta aktörer och forma samverkan. Ett nätverk är Cybercampus Sverige. Ett annat nätverk är samverkansplattformen Cybernoden – Sveriges nationella kompetensgemenskap inom cybersäkerhetsforskning och innovation.[37]

35 Kompetensråd i Göteborgsregionen, https://kompetensrad.se/goteborgsregionens-kompetensrad/. [Hämtad 2024-02-22]
36 Nationella Vårdkompetensrådet, https://www.nationellavardkompetensradet.se/. [Hämtad 2024-02-14]
37 Cybercampus Sverige, https://www.cybercampus.se/; Cybernode. https://cybernode.se/. [Hämtad 2024-02-14]

6. Bild av kompetensbehovet

Behovet

I dag saknas en heltäckande bild av behovet av kompetensförsörjning inom cybersäkerhet. För att kunna gå in med rätt insatser och utforma relevanta utbildningar, behövs mer kunskap om vilka kompetenser som efterfrågas på svensk arbetsmarknad. Det behövs kunskap om hur stora behoven är samt hur befintliga kompetensförsörjnings- och utbildningsinsatser möter behoven. För att öka förståelsen för kompetens- och utbildningsbehovet, behövs också en ökad samsyn om vilka kompetenser som faktiskt ingår i olika roller och yrkestitlar inom cybersäkerhetsområdet.

Vår lösning

Ett första steg för att på sikt kunna kartlägga kompetensbehovet mer systematiskt är att identifiera centrala yrkesroller inom cybersäkerhet. I relation till rollerna behöver man beskriva vilka förmågor och kompetenser som generellt är efterfrågade. Arbetet med att ta fram definitioner bör ske i bred samverkan mellan viktiga aktörer inom utbildning och akademi samt arbetsgivare i privat och offentlig sektor.

Gemensamma definitioner underlättar arbetet med att utforma utbildningar och forskningsinsatser, liksom rollbeskrivningar i arbetslivet. Det kan skapa en bättre matchning mellan utbildningars innehåll och arbetslivets behov, vilket i sin tur kan underlätta och förbättra arbetsgivares rekryteringar. Tydligare definitioner av både yrkesroller och utbildningars innehåll kan också underlätta den statistisk uppföljningen av yrkesverksamma inom cybersäkerhet, där de yrkesaktiva på sikt enklare kan fångas upp.

Vad behöver vi göra?

För att definiera roller och kompetenser inom cybersäkerhet krävs ett projekt, där aktörer inom bransch och näringsliv, utbildningsanordnare och berörda myndigheter samarbetar. En lämplig samordnare bör utses för att samordna ett sådant projekt.

Goda exempel och pågående insatser

För att definiera roller och kompetenser finns redan befintliga ramverk att utgå från. Till exempel har EU:s cybersäkerhetsbyrå ENISA tagit fram European Cybersecurity Skills Framework (ECSF) bestående av 12 yrkesrollsprofiler inom cybersäkerhet.[38] Via ENISA och andra EU-nätverk finns också möjlighet till samverkan. Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) på MSB är en part som kan ta initiativ och förmedla kontakter.[39]

Det finns möjlighet att använda liknande uppföljning som andra EU-länder. ENISA arbetar bland annat med att sammanställa rapporter som underlag inför gemensamma europiska initiativ. Likaså byggs globala plattformar för att dela data och samverka.[40]

Statistisk uppföljning kan kopplas till ett pågående utvecklingsarbete inom Myndighetssamverkan för kompetensförsörjning och livslångt lärande, där deltagande myndigheter undersöker hur de bättre ska kunna prognostisera tillgång och efterfrågan på svensk arbetsmarknad i framtiden.

38 ENISA. ECSF. *European cybersecurity skills framework*, https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework. [Hämtad 2024-01-25]
39 MSB. *Nationellt samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE)*, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-samordningscenter-for-forskning-och-innovation-inom-cybersakerhet/. [Hämtad 2024-02-15]
40 Se till exempel European Commission. *European Cybersecurity Atlas*, https://cybersecurity-atlas.ec.europa.eu/. [Hämtad 2024-02-14]

Avslutande reflektioner

Förslagen som presenteras i den här rapporten fokuserar i hög grad på utbildningsaktiviteter. Med tanke på behovet av kunskapshöjning och den stora efterfrågan på spetskompetens är sådana aktiviteter av stor vikt. Alla kompetensförsörjningsproblem inom cybersäkerhet går dock inte att utbilda bort, inte minst eftersom det finns ett begränsat antal presumtiva studenter och arbetstagare inom cybersäkerhet i Sverige. Därför behöver det också finnas en öppenhet för mer organisatoriska lösningar, särskilt för arbetsgivare som har svårt att konkurrera om arbetskraft och rekrytera rätt kompetens. Till exempel finns skäl att undersöka om organisationer dels kan dela på sin spetskompetens, dels på ett mer systematiskt sätt kan utbyta erfarenheter och goda exempel.

Våra förslag handlar också mycket om att öka en grundläggande kompetens inom cybersäkerhet, både bland allmänheten och yrkesverksamma. På kort sikt är det avgörande för att hantera säkerhetshoten. Men vi behöver också främja digital spetskompetens inom cybersäkerhet – med specialisering och excellens i fokus. Vi behöver till exempel satsa på forskning och innovation, för att kunna bygga säkrare tekniska och organisatoriska system. På så sätt kan vi minska digitala risker långsiktigt.

Kompetensförsörjningen inom cybersäkerhet är ett framtidsinriktat arbete. Efterfrågan på kunskap förmodas bara öka, vilket kommer kräva fler insatser över tid. Nya direktiv och lagar tillsammans med förändringar i cyberhoten ökar kraven på både privata och offentliga organisationer att höja sin kompetensnivå. Förändringarna ställer också krav på oss att få en gemensam syn på vad de nya förutsättningarna innebär, hur vi bäst kan hantera dem samt vilka strukturer och regleringar som behöver komma till för att stötta en stärkt resiliens för digital säkerhet i Sverige.

Att stärka kompetensförsörjningen är ett gemensamt ansvar. Betydelsen av samordning och gemensam riktning diskuterades ofta både inför och under workshoppen som ligger till grund för förslagen i den här rapporten. Därmed har vi också formulerat förslagen med tillägg om att lämpliga aktörer behöver få i uppdrag att samordna insatserna och få ekonomiska förutsättningar att göra det. Här spelar regeringen en avgörande roll i att skapa förutsättningarna och fördela ansvaret till lämpliga myndigheter. Det bör dock betonas att olika samhällsaktörer själva bär ett stort ansvar för att genomföra insatserna och behöver prioritera initiativ som kan stärka kompetensförsörjningen inom cybersäkerhet.

03

REFERENSER OCH BILAGOR

Referenser

Rapporter och publikationer

Ahmed, A, Mattsson, O. *Nationell kompetensförsörjning inom it-, informations- och cybersäkerhetsområdet*. KnowIT, 2023.

Ansari, Meraj Farheen and Dash, Bibhu and Sharma, Pawankumar and Yathiraju, Nikhitha. "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review (September 2022)." *International Journal of Advanced Research in Computer and Communication Engineering* 2022.

Arbetsförmedlingen. *Långsiktig yrkesområdesanalys. Data/it.* Arbetsförmedlingen, 2023.

DESI. *Index för digital ekonomi och digitalt samhälle (Desi) 2022 Sverige*. Europeiska kommissionen, 2022.

ENISA. *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education.* ENISA, 2021.

ENISA. *Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU.* ENISA, 2021.

Gunnar Karlsson, Paola Lundén. *Agile Education Imagined: A report from the Cybercampus workshop on Agile Education*. KTH TRITA-EECS-RP 2023:1, January 2023.

ISC2. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. ISC2 Cybersecurity Workforce Study, 2023.

IVA. *Cybersäkerhet för ökad konkurrenskraft*. Kungl. Ingenjörsvetenskapsakademin, 2022.

MSB. *Kompetens inom informations-och cybersäkerhet. En förstudie om kompetensförsörjning för samhället*. Myndigheten för samhällsskydd och beredskap, 2021.

OECD. *OECD Reviews of Digital Transformation: Going Digital in Sweden*. OECD, 2018.

PaloAlto. UNIT 42, Attack Surface Threat Report. PaloAlto 2023.

Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Lendak, I., & Janout, V. Understanding Cybersecurity Education Gaps in Europe. *IEEE Transactions on Education*, 2024, 1–12.

SOFF. *"Vilka kompetenser och färdigheter söker Sveriges säkerhets- och försvarsföretag?" En rapport om vilka cyberkompetenser SOFF:s medlemsföretag inom cyberområdet efterfrågar.* Säkerhets- och försvarsföretagen, 2022.

Svenskt Näringsliv. *Företagen och IT-säkerheten – hotbilder, motåtgärder och behov.* Svenskt Näringsliv, 2021.

TechSverige. *Kompetensbehoven inom tech.* TechSverige, 2024.

TechSverige. *Techbranschens förslag för att möta cyberhoten.* TechSverige*, 2023.*

Tillväxtverket. *Säker digitalisering i små och medelstora företag. Kartläggning av behov och initiativ på marknaden.* Tillväxtverket, 2021.

Digitala källor

AI Competence for Sweden, https://ai-competence.se/. [Hämtad 2024-02-05]

Cybercampus Sverige https://www.cybercampus.se/. [Hämtad 2024-01-25]

Cybernode. https://cybernode.se/. [Hämtad 2024-02-14]

ENISA. *ECSF. European cybersecurity skills framework.* https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework. [Hämtad 2024-01-25]

European Commission. *Cyber Resilience Act.* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. [Hämtad 2024-02-15]

European Commission. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. [Hämtad 2024-02-15]

European Commission. *European Cybersecurity Atlas*, https://cybersecurity-atlas.ec.europa.eu/. [Hämtad 2024-02-14]

Hackschield https://se.joinhackshield.com/sv. [Hämtad 2024-02-01]

Högskolan Väst. *Introduktion till industriell cybersäkerhet*, https://www.hv.se/utbildning/kurs/introduktion-till-industriell-cybersakerhet-deltid-distans-iic600/. [Hämtad 2024-02-14]

Internetstiftelsen. *Kunskap.* https://internetstiftelsen.se/kunskap/. [Hämtad 2024-02-01]

IT-högskolan. *IT-säkerhet, YH-kurs*. https://www.iths.se/utbildningar/it-sakerhet/. [Hämtad 2024-02-14]

KK-stiftelsen. *Expertkompetens*, https://www.kks.se/program/expertkompetens/. [Hämtad 2024-02-14]

Kompetensråd i Göteborgsregionen, https://kompetensrad.se/goteborgsregionens-kompetensrad/. [Hämtad 2024-02-22]

Learning 4 professionals, *Öppet för klimatet*, https://learning4professionals.greentown.se/oppet-for-klimatet/. [Hämtad 2024-02-05]

Minecraft Education https://education.minecraft.net/en-us/discover/cyber-and-digital-safety. [Hämtad 2024-02-01]

MSB. *Kurser i informationssäkerhet.* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/kurser-i-informationssakerhet/. [Hämtad 2024-02-15]

MSB. *Nationellt samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE)* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-samordningscenter-for-forskning-och-innovation-inom-cybersakerhet/. [Hämtad 2024-02-15]

MSB. *Tänk säkert*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/tank-sakert/. [Hämtad 2024-02-01]

Myndigheten för psykologiskt försvar. *Bli inte lurad*. https://www.bliintelurad.se/. [Hämtad 2024-02-01]

Nationella Vårdkompetensrådet, https://www.nationellavardkompetensradet.se/. [Hämtad 2024-02-14]

Regeringskansliet. *Regeringen satsar på svenskt cybercampus vid KTH.* https://www.regeringen.se/pressmeddelanden/2023/09/regeringen-satsar-pa-svenskt-cybercampus-vid-kth/. [Hämtad 2024-01-25]

Regeringskansliet, *Korta kurser för yrkesverksamma som vill vidareutbilda sig eller ställa om i yrkeslivet ska stärka kompetensförsörjningen för den gröna omställningen.* https://www.regeringen.se/pressmeddelanden/2023/12/korta-kurser-for-yrkesverksamma-som-vill-vidareutbilda-sig-eller-stalla-om-i-yrkeslivet-ska-starka-kompetensforsorjningen-for-den-grona-omstallningen/. [Hämtad 2024-02-22]

Vinnova. *Samverkan för livslångt lärande – Uppdragsutbildning*, https://www.vinnova.se/p/samverkan-for-livslangt-larande---uppdragsutbildning/. [Hämtad 2024-02-14]

Bilaga 1 – SWOT-analys

Nedan presenteras en SWOT-analys, som sammanfattar de styrkor (S), svagheter (W), möjligheter (O) och hot (T) som finns kopplat till kompetensförsörjning inom cybersäkerhet. Analysen är främst baserad på synpunkter som lämnats från deltagare på konferensen om kompetensförsörjning inom cybersäkerhet 2023. Även resultat från en övergripande omvärldsanalys har vägts in.

Styrkor

1. **Frågans aktualitet skapar medvetenhet, attraktivitet och möjliggör kraftsamling.** Att cybersäkerhet är en sådan högaktuell fråga gör att kompetensförsörjningen inom området blir en prioriterad fråga. Det skapar också en attraktivitet för branschen, där samhällsnyttan kan locka fler studenter och yrkesverksamma. Likaså möjliggörs en kraftsamling, där aktörer från olika aktörer får motivation att komma samman och hitta gemensamma lösningar.
2. **Hög kompetens i Sverige**. Vi har kommit långt i Sverige inom både digitalisering och cybersäkerhetskompetens. Även om bristen på kompetens är stor finns det mycket kompetenta personer på viktiga nyckelfunktioner i svenska organisationer.
3. **Bra grund i utbildningssystemets utbud och studiemöjligheter**. I grunden finns ett bra utbud av utbildningar, inte minst inom tekniska inriktningar. Likaså har Sverige ett stabilt system för att möjliggöra studier, till exempel genom studiefinansiering.
4. **Goda exempel på alternativa karriärvägar.** Det finns flera exempel på företag som till exempel arbetar med traineeprogram för att stärka junior kompetens. Likaså finns många olika typer av yrkesutbildningar och certifieringar.

Svagheter

1. **Otydlig behovsbild, bristande statistik och avsaknad av definitioner.** Vi vet för lite om hur det faktiska kompetensbehovet ser ut. Utifrån befintlig statistik är det svårt att fånga upp vilka som arbetar inom fältet, hur arbetsgivare bedömer kompetensbehov, vilket utbildningsutbud som finns och vilka som studerar. Cybersäkerhet går in i flera olika områden, vilket försvårar statistiska mätningar. Det saknas även en gemensam syn på roller och titlar. Till exempel är det inte fastställt vad en ”specialist” inom området är.
2. **Brist på specialistkompetens och erfarenhet.** Det är väldigt hög konkurrens om kompetens och resurser. Det skapar en hög belastning på organisationer. Eftersom det ofta är spetskompetens som efterfrågas blir rekryteringen särskilt svår. Det blir långa ledtider för att få fram en kompetens som egentligen behövs redan i dag.
3. **Otydliga utbildnings- och karriärvägar**. Även om allt fler utbildningar skapas finns en oro inför att utbudet blir väldigt spretigt med många olika aktörer som erbjuder olika typer av innehåll och inriktningar. Utbildningarna är inte standardiserade, vilket gör att en arbetsgivare till exempel inte vet vad en utbildning faktiskt ger för kompetens.
4. **Avsaknad av helhetsperspektiv**. Inom cybersäkerhetsområdet råder fortfarande ett stort fokus på teknik, vilket gör att många roller som är centrala för arbetet med cybersäkerhet hamnar i skymundan. Det berör till exempel jurister, pedagoger och organisationsvetare. Samma teknikfokus syns även till viss del i utbildningsutbudet. Det saknas ett helhetsperspektiv, där teknik kopplas samman med samhällsprocesser och människa.
5. **Ojämn könsfördelning.** Inom data- och it-området i stort råder en skev könsfördelning, där män är i stor majoritet både bland yrkesverksamma och studenter.

6. **Brist på samordning och politisk riktning.** Frågan berör många sektorer och därmed också departement. Insatser sker men inte samordnat.

Möjligheter

1. **Ökat inslag av cybersäkerhet i hela utbildningskedjan**. Cybersäkerhet behöver bli en närvarande fråga från grundskolan till forskarutbildningen. Skälet är att vi behöver skapa medvetenhet och intresse från tidiga åldrar som därefter kan byggas på och utvecklas.
2. **Stärkt utbud av eftergymnasial grundutbildning.** Mer konkret ges förslag på fler utbildningsplatser och mer resurser för utbyggnad, framför allt inom högskolan.
3. **Stärkt utbud för omställning och vidareutbildning.** För att möjliggöra livslångt lärande krävs ett utbud som passar redan yrkesverksamma. Eftersom många är yrkesverksamma inom data- och it-området finns en stor ”pool” att rekrytera från till den typen av utbildningsinsats. Här är också omställningsstudiestödet en möjliggörare. Även intern kompetensutveckling kan kopplas till den möjligheten.
4. **Cybersäkerhet i andra utbildningsinriktningar**. Cybersäkerhet behöver bli en naturlig del i andra ämnesområden, för att möjliggöra ett helhetsperspektiv.
5. **Samverkan näringsliv och utbildningssektor**. Näringslivet behöver bli involverat i utformandet av utbildningar, för att säkerställa att utbildningarna lever upp till branschens behov och kan anpassas efterhand. Det efterfrågas även fler praktiska inslag i utbildningarna, där näringslivet kan vara en viktig möjliggörare.
6. **Kompetensprofiler och statistik**. Att enas om definitioner av yrkesroller och titlar är ett första steg, för att därefter kunna utveckla statistiken och undersöka hur den kan användas för att följa upp kompetensbehov och utbildningsutbud. Gemensamma definitioner och profiler kan även underlätta utbildningsplanering och rekrytering.
7. **Traineeprogram och alternativa lösningar**. Kompetensutmaningarna inom cybersäkerhetsområdet kan inte bara lösas med nya deltagare på grundutbildningar. Vi måste tänka på andra parallella spår, till exempel traineeprogram.

Hot och risker

1. **Ökade cyberhot och ökad digital sårbarhet.** Ökade risker kan leda till ännu större kompetensbehov, och därmed ökad kompetensbrist.
2. **Global konkurrens om arbetskraft och resurser**. Efterfrågan på kompetens inom cybersäkerhetsområdet är global. För att kunna vara attraktiv för spetskompetens behöver konkurrenskraften vara spetsat.
3. **Säkerhetsklassning begränsar talangpoolen**. En verklig utmaning för många rekryteringar är de hårda säkerhetskraven som ofta ställs för att få arbeta inom cybersäkerhetsområdet. De särskilda krav som ställs (till exempel svenskt medborgarskap) kan begränsa rekryteringar till tjänster och lärarpositioner. Internationell talangattraktion är därmed inte alltid en möjlig lösning.
4. **Bristande intresse för utbildning**. Om det finns bristande intresse eller möjligheter att studera, riskerar en utbyggnad av utbildningsplatser och satsningar på vidareutbildning att falla platt.
5. **Silo-tänk där cybersäkerhet blir en teknisk fråga**. Om cybersäkerhet inte integreras och ses som en organisatorisk fråga, finns en risk att vi inte kan hantera cybersäkerhetshoten.
6. **Ekonomi och prioriteringar.** Som med alla frågor finns det organisatoriska utmaningar i att genomföra förändringar. Många satsningar för att stärka kompetensförsörjning inom cybersäkerhet kräver finansiering, men i en ansträngd ekonomi finns en risk att finansiering inte tillförs.