



Policy för att främja utbildning, forskning och ökad medvetenhet om cybersäkerhet

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras i det vidare arbetet med policyn.

1 Nulägesbild

1.1 Cybersäkerhetsutbildning och cybersäkerhetskompetens

Europeiska företag upplever stora svårigheter med att rekrytera lämpliga kandidater till lediga tjänster, och bristen på cybersäkerhetskompetens utgör ett väsentligt bekymmer. Majoriteten av personer i cybersäkerhetsrelaterade roller har inte formell utbildning eller certifiering inom området. EU:s cybersäkerhetsbyrå, ENISA, identifierar kompetensbristen som ett av de tio största hoten och en av framtidens stora utmaningar inom cybersäkerhet. Särskilt lyfts bristen på jämställdhet inom området, en undersökning visar att majoriteten av tillfrågade företag anser att mångfald och inkludering inom cybersäkerhet är viktigt i organisationen, samtidigt som hälften av de svarande inte har några kvinnor anställda på området.

Det finns flera EU-initiativ som syftar till att främja kompetensförsörjning inom cybersäkerhet och Sverige deltar aktivt, framför allt kring det europeiska ramverket för cybersäkerhetskompetens, ECSF, och den europeiska kompetensakademien för cybersäkerhet, Cyber Skills Academy.

Kompetensbehovet i Sverige

Läget i Sverige speglar den europeiska bilden. Ett antal olika undersökningar och analyser gjorts i Sverige avseende kompetensförsörjning inom informations- och cybersäkerhetsområdet, med samstämmiga resultat: behovet av kompetens på området kommer att fortsätta öka samtidigt som svårigheterna att hitta personal som kan möta behoven redan idag är betydande. Även i Sverige finns en könsobalans där kvinnor är väsentligt underrepresenterade på cybersäkerhetsrelaterade tjänster.

Gemensamt för resultaten av gjorda undersökningar är också att de pekar på svårigheterna i att beräkna både arbetsmarknadens behov och utbildningsväsendets försörjning av relevant kompetens. En central utmaning är att kompetenser inom informations- och cybersäkerhet benämns på många olika sätt. Detta gäller dels i hur olika roller och

förmågor beskrivs hos organisationerna på arbetsmarknaden, dels i hur utbildningsaktörer beskriver de färdigheter som ingår i olika utbildningsalternativ. Bilden blir än mer komplex genom att arbetet ofta är tvärfunktionellt och kräver en kombination av kompetenser från olika områden, samtidigt som behoven varierar beroende på verksamhetens art och vilka legala krav den omfattas av.

Utbildningsutbudet

Utbudet av utbildningar inom cybersäkerhetsområdet är relativt brett, både avseende innehåll, format och målgrupper. Såväl universitet och högskolor som yrkeshögskolor erbjuder längre utbildningsprogram samt kortare kurser. Kurserna ges dels inom ramen för andra program, exempelvis juridik, dels som fristående alternativ. Fristående kurser tillhandahålls även av kommersiella aktörer, och fokuserar ofta på snabb kompetensutveckling för redan yrkesverksamma, för att matcha den snabba utvecklingen inom ämnesområdet.

Det finns också en stark utveckling av kommersiella certifieringar av individuell kompetens. I den flora av olika kurser och utbildningar som finns på området, där det är svårt att värdera vilken kompetens de resulterar i, blir internationella certifieringar attraktiva som kompetensbenämningar för både arbetsgivare och för den som utbildar sig.

Samtidigt finns utmaningar med att kartlägga de utbildningsmöjligheter som finns inom området, även här på grund av brist på enhetliga benämningar men också begränsade sökmöjligheter för utbildningar inom vissa typer av lärosäten eller kurser som ingår i bredare program med annan inriktning. En annan problematik är att informations- och cybersäkerhet ofta erbjuds som valbara kurser eller inriktningar, och det saknas samlad statistik över hur många som väljer dessa kurser eller hur många som examineras från sådana inriktningar.

Initiativ för ensnig av benämningar

Svårigheten att kartlägga såväl kompetensbehovet på arbetsmarknaden som utbildningsutbudet gör det svårt att sammanställa en tydlig bild av var gapen faktiskt finns.

Flera undersökningar har prövat att tillämpa ENISA:s cybersecurity skills framework (ECSF) som ramverk för beskrivning av roller och kompetenser på cybersäkerhetsområdet, och mappa det till det svenska utbildningsutbudet. Ramverket täcker olika typer av roller med tekniska, juridiska och ledningsnära aspekter av cybersäkerhetsarbetet. Undersökningarna bedömer att ramverket är relevant och har en enkel struktur men kan behöva anpassas för svenska förhållanden för att fullt ut möta behoven från både arbetsmarknads- och utbildningssynpunkt. Bland annat efterfrågas koordinerade roller som informationssäkerhetssamordnare särskilt i Sverige.

Utbildning på lägre nivå

Inom grundskola och gymnasium blir digitala verktyg och navigering i den digitala miljön allt mer centrala verktyg i kunskapsutvecklingen, medan säkerhetsaspekter är ett mestadels utvecklat område i undervisningen.

Flera organisationer tillhandahåller material som kan användas i skolan på olika nivåer, och/eller erbjuder aktiviteter och utbildning på fritiden för barn och ungdomar; bland

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

annat Unga forskare, Kodcentrum, Internetstiftelsen och Stölskyddsföreningen. Olika typer av spelaktiviteter, hackatons och andra initiativ förekommer också, i syfte att öka intresset för ämnet.

1.2 Forsknings- och utvecklingsinitiativ

Forskning och utveckling går mot mer tvärvetenskapliga horisontella satsningar med fokus på en ständigt uppkopplad värld, intelligenta sammankopplade system och ökat fokus på beräkningskapacitet och data samt att få ut lösningar på marknaden. Den snabba digitala utvecklingen och de risker som följer med den ställer ökade krav på information- och cybersäkerhet i digitala system, vilket manifesterar sig i form av ny europeisk lagstiftning och ökade satsningar på forskning och utveckling. Inrapporterade incidenter till MSB indikerar att ändringshantering och organisationers systematiska cybersäkerhetsarbete är bristområden.

I Sverige finns det ett nationellt ekosystem för insatser som stöd för forskning och utveckling inom cybersäkerhet. Traditionellt bedriver universitet och högskolor forskning, innovation och utbildning. På senare år har insatser gjorts för att underlätta samarbete mellan näringsliv och akademi i syfte att främja kunskapsutveckling och överbrygga eventuella gap till marknad. Detta återspeglar sig både i EU:s finansieringsprogram så väl som i nationella initiativ.

Nationellt ser vi betydande insatser och ökade aktiviteter och anslag via aktörer så som Myndigheten för samhällsskydd och beredskap, Vinnova, Vetenskapsrådet, Myndigheten för digital förvaltning, Tillväxtverket med flera. Ett etablerat initiativ är Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) med uppdrag att främja samarbete mellan forskningsinstitut, företag och offentlig sektor för att skapa bättre cybersäkerhetslösningar. Utöver detta finns initiativ så som till exempel Cybernoden och Cybercampus. Cybernoden är en nationell kraftsamling kring cybersäkerhet för att accelerera forskning och innovation inom industri och offentlig sektor. Cybercampus Sverige är en nationell satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige. Ytterligare ett initiativ är Sweden Secure Tech Hub, ett delvis EU-finansierat samarbete mellan sex av Sveriges ledande science parks inom tech och digitalisering. Andra initiativ som stöttar forskning och utveckling inom cybersäkerhet är Knut och Alice Wallenbergs Stiftelse liksom Internetstiftelsen, Stiftelsen Tryggare Sverige och Unga Forskare för att nämna några.

Gällande finansiering så finns det möjlighet för svenska aktörer att delta i forskning och utveckling i samverkan med andra länder i de stora europeiska finansieringsprogrammen så som till exempel Horisont Europa och Programmet för ett digitalt Europa (DIGITAL). Horisont Europa gör det möjligt för länder och aktörer att gemensamt ta fram vetenskapligt underbyggd kunskap och innovativa lösningar. Cybersäkerhet som område ligger inom kluster 3: Civil säkerhet för samhället som fokuserar på insatser för att stödja EU:s tekniska kapacitet, bidra till att skydda infrastrukturer och stödja europeisk konkurrenskraft. Programmet för ett digitalt Europa är utformat för att stödja införandet av avancerad digital teknik och överbrygga klyftan mellan forskning om digital teknik och marknadsutnyttjande. Inom cybersäkerhet fokuserar det nuvarande programmet på ny

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

teknik, cybersolidaritetslagen och det europeiska varningssystemet för cybersäkerhet och hantering av cybersäkerhetskriser liksom genomförande av lagstiftning som syftar till att öka EU:s motståndskraft.

Svenska aktörer kan söka finansiering inom europeiska program och nationella aktörer som stöttar forskning och utveckling, till exempel:

- EU:s program för ett Digitalt Europa, arbetsprogram cybersäkerhet
- EU:s program Horisont Europa, kluster 3 Civil säkerhet för samhället
- Vinnova, programmet Avancerad digitalisering
- Vetenskapsrådet, utlysningar inom området naturvetenskap och teknikvetenskap
- Stiftelsen för Strategisk Forskning, cyberresilienta AI-system
- MSB via NCC-SE, finansiellt stöd till tredje part (FSTP) för små och medelstora företag

Några exempel på områden inom cybersäkerhet där det bedrivs forskning och utveckling i Sverige:

- IoT / OT-säkerhet med fokus på säkerhet i sammankopplade system, sårbarheter och drift.
- AI och automatisering – både som möjliggörare och som risk. Hur AI kan användas för att upptäcka hot men också hur AI själv kan bli en attackyta.
- Informationssäkerhet/riskhantering/reglering – hur organisationer styr sitt säkerhetsarbete
- Tekniska infrastrukturer och testmiljöer – så som cyber range, testbäddar, demonstrationsmiljöer för att pröva nya säkerhetslösningar
- Cybersäkerhet inom 5G-teknologi och trådlös kommunikation
- Kryptografiska tekniker – ny generation kryptografiska algoritmer designade för att stå emot angrepp från både klassiska datorer och framtida kvantdatorer.
- Security by design och zero trust-arkitektur
- Cybersäkerhet i teknologier eller produkter som kan användas både för civila och militära ändamål
- Integritetsförbättrande teknologier (PET)

1.3 Cyberhygien och medvetandehöjande åtgärder

Samhällets försvar mot cyberhot och cyberattacker är beroende av att Sveriges befolkning har en allmän cybersäkerhetkompetens. Med en ständigt accelererande teknisk utveckling och mer sofistikerade cyberattacker ökar behovet av medvetandehöjande åtgärder och ökad kunskap om cyberhygien hos allmänheten. Cyberhygien är åtgärder som skyddar oss från cyberhot, för allmänheten innebär det att skydda sin personliga information och sina digitala enheter.

ENISA Threat Landscape 2024 report lyfter incidenter som riktas mot det civila samhället och allmänheten genom social manipulering, dataläckor och påverkanskampanjer. ENISA

konstaterar att hälften av EU-medborgarna saknar den digitala kompetens som behövs för att fullt ut kunna delta i samhället, vilket hindrar deras tillgång till tjänster som tillhandahålls online. Undersökningar visar bland annat att olika sociodemografiska grupper har olika nivåer av digital kompetens och att medvetenheten är låg när det gäller cyberbrottslighet och vilka rapporteringsmekanismer som finns för allmänheten.

Sveriges förutsättningar för att främja medvetenhet och god cyberhygien skiljer sig delvis från det europeiska genomsnittet:

- Sverige har ett högt deltagande i det digitala livet. År 2025 använder 97 procent av svenskarna (16 år eller äldre) internet. Den dagliga användningen av internet når i år 93 procent vilket är en liten ökning mot föregående år. I princip alla födda på 60-talet eller senare är på nätet varje dag. Ålder är den faktor som har störst påverkan på internetanvändandet då det i princip uteslutande är svenskar i pensionsåldern som inte är på nätet.
- Sverige anses ligga över medel i EU vad gäller medborgares medvetenhet om god cyberhygien.
- Invånare i Sverige har hög digital kompetens jämfört med EU, särskilt bland yngre.
- Sverige har flera långsiktiga och etablerade insatser för kunskaps- och medvetandehöjning bland befolkningen.
- I Sverige finns hos offentliga aktörer, privata företag, branschorganisationer och föreningar ett brett engagemang för att öka befolkningens cybersäkerhet, och en stor vilja för samarbete mellan dessa parter.
- Sverige har god samverkan mellan myndigheter och medborgare.
- Det finns i Sverige fortfarande ett gap mellan olika grupper i samhället, där ålder är den viktigaste faktorn men även stad/landsbygd påverkar. Sverige följer här EU-mönstret vad gäller klyftor i den digitala kompetensen.
- Flera svenska undersökningar visar att medvetenheten om cyberbrott höjts och när det gäller risken att utsättas för digitala brott ökar oron. Utvecklingen mot ett säkrare beteende går dock långsamt och inte i takt med den digitala utvecklingen i samhället. Även i övriga EU har invånarnas tilltro till sin förmåga att skydda sig mot cyberbrott minskat, vilket tyder på att medvetenheten om cybersäkerhet sannolikt har ökat bland EU-medborgarna.

Tänk säkert-kampanjen

Varje år i oktober genomför MSB, Polisen och drygt 20 andra organisationer från privat sektor, offentlig sektor och föreningslivet gemensamt kampanjen Tänk säkert, för att öka medvetenheten och kunskapen om informationssäkerhet för allmänhet och små företag. Kampanjen stöts av regeringen och har genom samarbeten nått ett brett genomslag i samhällets olika delar, och även om den drivs en månad om året finns utbildningar och informationsmaterial där besökare kan fortbilda sig årets runt.

Kampanjen uppfyller i princip alla delar som Enisa har satt upp för medvetenhetshöjande insatser i sin Capability assessment för cyberhygien och medvetenhet, med två undantag: Kampanjer genomförs inte ad hoc, det vill säga i efterdyningarna av en cyberincident och i

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

kampanjen Tänk säkert ingår inte beteendevetare för att maximera effekten ut mot specifika målgrupper.

Andra folkbildande initiativ

Utöver Tänk säkert genomförs även årliga informationssäkerhetsinsatser av andra aktörer. Ett exempel är kampanjen Svårlurad som är en gemensam kampanj från Sveriges banker. Ett annat är Digitalidag som samlar aktörer över hela Sverige och når runt en miljon människor under en dag i oktober varje år, med kunskapshöjande aktiviteter som höjer den digitala delaktigheten och säkerhetsmedvetenheten. Gemensamt för alla initiativen är att de sker i samverkan mellan flera olika parter, oftast från både offentlig och privat sektor.

Säkerhetskollen - ett initiativ från Stöldskyddsföreningen

Säkerhetskollen är en webbplats där invånare och företagare kan fortbilda sig inom cybersäkerhet, och som skickar ut varningar om pågående digitala brott. Stöldskyddsföreningen arbetar aktivt med polis, myndigheter, försäkringsbolag och banker för att ligga i framkant i kampen mot den digitala brottsligheten.

Internetstiftelsen

Internetstiftelsen tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och digital säkerhet. Internetstiftelsen vänder sig till allmänheten, men särskilt till äldre och yngre. Bland annat har de utvecklat digitala lektioner som används i skolorna.

2 Analys

2.1 Cybersäkerhetsutbildning och cybersäkerhetskompetens

Det är positivt att frågan om kompetensförsörjning finns på dagordningen och uppmärksammas genom olika initiativ och undersökningar. EU-utveckling pågår i flera spår på området. Aktörer från olika samhällssektorer är aktiva och redo att verka för förändring, vilket ger bra förutsättningar för gemensamma insatser med brett stöd.

Det är också en styrka att det finns ett stort och varierat utbildningsutbud från olika typer av aktörer vilket gör det möjligt för dem som vill att yrkesutbilda sig, fortbilda sig eller komplettera en annan utbildning. På så sätt kan kompetens tillföras marknaden på olika sätt och på ett individuellt plan kan det ske i flera skeden av en yrkesbana.

I fråga om kompetensförsörjning ligger den övergripande utmaningen i det faktum att samtidigt som efterfrågan på personer med cybersäkerhetskompetens ökar snabbt, växer också bristen på människor med rätt kompetens som kan fylla behoven. Detta leder till flera problem, bland annat att företag, myndigheter och andra organisationer får svårt att upprätthålla ett tillfredsställande arbete med cybersäkerhet, vilket gör dem mer sårbara för störningar i verksamheten som kan drabba både kunder/medborgare/användare och uppdragsgivare. En annan konsekvens är att arbetsmarknaden snedvrids då den eftertraktade kompetensen samlas hos de arbetsgivare som upplevs erbjuda de mest

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

attraktiva villkoren, med följderna att andra får än större svårigheter att rekrytera till kritiska roller.

Orsakerna till kompetensbristen finns på olika plan. Allt för få intresserar sig för ämnet, det uppfattas som tekniskt, svårt och abstrakt och många kommer främst i kontakt med det genom incidenter, vilket ofta väcker negativa associationer snarare än ett intresse för området som en möjlig yrkesväg. Kvinnor förefaller vara särskilt ointresserade av ämnet. Säkerhetsaspekter tas inte upp som en naturlig del av digital kompetens i skolundervisning eller i samhället i stort. Det stora antalet utbildningsalternativ ger en otydlig bild av karriärmöjligheter och framtidsutsikter.

En central svårighet med att främja och underlätta kompetensförsörjningen ligger i bristen på detaljerad information, om behoven och tillgången på kompetens samt hur mycket kompetens som kan tillföras genom utbildningar. Avsaknaden av gemensamma beskrivningar för roller och kompetenser inom cybersäkerhet, såväl ur arbetsgivar- som utbildarperspektiv, försvårar både matchning, jämförelser och behovsbedömningar. I kombination med en bristfällig helhetsbild av den utbildningskapacitet som finns blir det mycket svårt att avgöra om utbildning finns inom rätt kompetenser i förhållande till behoven. Detta i sin tur försvårar beslut om vilka åtgärder som behöver vidtas, och även utvärdering av resultaten.

Mot den bakgrunden är det positivt att ett ramverk utvecklats på EU-nivå som syftar till att etablera en gemensam benämningsstruktur för cybersäkerhetskompetens, och att det enligt genomförda studier förefaller användbart för svenska förhållanden.

2.2 Forsknings- och utvecklingsinitiativ

Det positiva är att det finns aktörer och nätverk liksom tydliga satsningar inom cybersäkerhet, ett område med forsknings- och utvecklingsbehov i och med den ständigt accelererande tekniska utvecklingen och de mer sofistikerade cybersäkerhetsattacker. När samhällets behov ökar i och med den ökade graden av digitalisering och utifrån det rådande geopolitiska läget reagerar Sverige proaktivt på de globala utmaningar som cyberhot utgör och visar att Sverige är ett land som är medveten om de utmaningar som måste mötas under de kommande åren.

Det negativa är att Sverige trots satsningar på forskning och utveckling inom cybersäkerhet har väldigt få beviljade ansökningar inom EU:s stora finansieringsprogram Horisont Europa och DIGITAL i förhållande till sina europeiska grannländer. För att Sverige även fortsättningsvis ska vara ett framstående forsknings- och innovationsland och en ledande kunskapsnation behöver svenska aktörer i utökad grad delta även i europeiska projekt och bidra med sin kunskap och kompetens på den europeiska arenan. Att det har varit svårt för svenska aktörer att söka finansiering och delta kan i viss mån bero på nivån på krav om egen finansiering i forsknings- och utvecklingsprojekt liksom svårigheten i att skriva bra ansökningar. Intresset från svenska aktörer för att ansöka om EU-finansiering inom cybersäkerhet har hittills varit relativt lågt trots att det finns behov av finansiering. Aktörer som i behov av specifika insatser som pekats ut av EU är små och medelstora företag liksom kommuner och regioner.

Det är även negativt att nästan hälften av alla inrapporterade incidenter till MSB orsakas av misstag eller systemfel som hade kunnat förebyggas. Ändringshantering och organisationers systematiska cybersäkerhetsarbete är i många fall eftersatt liksom arbete för att förebygga digitala leveranskedjeincidenter samt arbetet med informationsdelning när incidenter väl har uppstått. En bidragande orsak till detta är att det saknas kunskap om hur effektiva verktyg och processer bör vara utformade.

2.3 Cyberhygien och medvetandehöjande åtgärder

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.

En befolkning med hög medvetenhet och stabila vanor inom cyberhygien är mer motståndskraftig mot cyberhot. Detta bidrar till en säkrare digital miljö för alla och möjliggör ett allmänt deltagande i den digitala tidsåldern samtidigt som det främjar ekonomisk tillväxt. Sveriges befolkning har ännu inte en tillräckligt hög medvetenhet och stabila vanor inom cyberhygien. Det innebär att individer själva, såväl som organisationerna där de är verksamma, är mer sårbara för cyberrisker än de hade behövt vara.

Det är visserligen positivt att Sverige ligger över genomsnittet i EU vad gäller digitalt deltagande, kunskap och medvetenhet, men deltagandet, den allmänna kunskapen och medvetenheten är trots det otillräcklig, i synnerhet i vissa grupper. Möjliga orsaker till klyftorna mellan olika grupper kan vara språkhinder men även funktionshinder i form av hörselnedsättning, synsvårigheter och inlärningssvårigheter. Andra faktorer kan vara vid vilken tidpunkt i livet personen introducerades i det digitala livet, och i vilken samhällelig kontext personen befinner sig i såsom utbildningsnivå, om personen har en anställning eller bostadsort.

Dessa grupper är svåra att nå genom allmänhetsundersökningar, eftersom detta kräver förmåga att svara på undersökningar via telefon eller webb. Personer som exempelvis har läs- och talsvårigheter eller av andra skäl inte kan svara eller nås, kan därför inte anses fullt belysta i någon undersökning och nås troligen inte av medvetandehöjande insatser i lika hög grad trots att det hos dessa grupper finns stora behov.

Klyftor mellan olika grupper när det gäller medvetenhet om cyberhygien kan leda till att vissa stängs ute från delar av samhället när tjänster går över till att bli enbart eller i stor utsträckning digitala, vilket både Internetstiftelsens och ENISA:s undersökningar pekar på. I slutändan kan detta påverka både människors livskvalitet och möjlighet att delta i vårt demokratiska samhälle.

Att både svenskar specifikt och EU-medborgare generellt uttrycker en större oro för att bli utsatta för cyberbrott än tidigare tyder dock på att medvetenheten om cyberrisker har ökat bland befolkningen, vilket bör innebära ökade förutsättningar för befolkningen att ta till sig vägledning och förbättra sin cyberhygien.

Sammantaget har Sverige flera positiva omständigheter som ett brett engagemang i frågorna, flera etablerade och effektiva initiativ och en kunskapsnivå hos befolkningen som är över genomsnittet i EU. Det kan dock också konstateras att vi även i Sverige

behöver ytterligare höja nivån på cyberhygien hos befolkningen i stort så att utvecklingen på säkerhetsområdet kan närma sig utvecklingen inom digitaliseringen och motsvara de krav som det säkerhetspolitiska läget ställer på samhället.

Referenser

Utbildning och kompetensförsörjning

European cybersecurity skills framework (ECSF), ENISA,
<https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf>

Cybersecurity skills academy, EU-kommissionen,
<https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy>

2024 report on the state of cybersecurity in the Union, ENISA,
<https://op.europa.eu/en/publication-detail/-/publication/e7d6ea3d-605a-11f0-a9d0-01aa75ed71a1/language-en>

Sex förslag för en stärkt kompetensförsörjning inom informationssäkerhet;
 Universitetskanslersämbetet, Tillväxtverket, Luleå tekniska universitet och MSB,
<https://www.myh.se/om-oss/myndighetssamverkan-och-samverkansprojekt/myndighetssamverkan/aktuellt-inom-myndighetssamverkan/sa-kan-kompetensforsorjningen-starkas-inom-cybersakerhet>
samt ett ännu ej publicerat fortsättningsprojekt.

Nationell kompetensförsörjning inom it-, informations- och cybersäkerhetsområdet,
 Knowit, <https://info.knowit.se/rapport-nationell-kompetensforsorjning>

Kompetensbehoven inom tech, TechSverige,
<https://techsverige.se/2024/02/ny-rapport-sverige-behover-arligt-tillskott-av-18-000-specialister-inom-tech-2/>

Cyberkompetensrapport, Säkerhets- och försvarsföretagen,
<https://soff.se/dokument/cyberkompetensrapport/>

Forskning och utveckling

Regeringens proposition 2024/25:60, Forskning och innovation för framtid, nyfikenhet och nytta,
<https://www.regeringen.se/contentassets/a70996e2f9de4222b5a6880d33c20d35/forskning-och-innovation-for-framtid-nyfikenhet-och-nytta-prop.-20242560.pdf>

Ändringar som både hotar och skyddar 20 rekommendationer för säkrare ändringar i våra informationssystem, MSB, <https://www.msb.se/sv/publikationer/andringar-som-bade->

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

[hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/](#)

Verktyg för ökad motståndskraft och stärkt civilt försvar: årsrapport it-incidentrapportering 2024, MSB, <https://www.msb.se/sv/publikationer/verktyg-for-okad-motstandskraft-och-starkt-civilt-forsvar--arsrapport-it-incidentrapportering-2024/>

RESEARCH AND INNOVATION BRIEF Annual Report on Cybersecurity Research and Innovation Needs and Priorities MAY 2022, ENISA, <https://www.enisa.europa.eu/sites/default/files/publications/RIT%20Annual%20Report%202021.pdf>

2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION, ENISA, <https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf>

Europe's Digital Decade: digital targets for 2030, https://commission.europa.eu/europes-digital-decade-digital-targets-2030-documents_en

Horizon Europe Work Programme 2025, 6. Civil Security for Society, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf

ECCC Digital Europe Cybersecurity Work Programme 2025-2027, https://cybersecurity-centre.europa.eu/document/download/8af166e1-69c5-4ccd-b38f-5a3ffe43ad73_en?filename=DEP%20WP2025-2027_March2025.pdf

Cyberhygien och medvetandehöjande åtgärder

Svenskarna och internet 2025, Internetstiftelsen, <https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2025/>

State of the Cybersecurity in the Union 2024, ENISA, <https://enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

IT-SÄKERHET 2024 Allmänhetens beteenden och inställningar till frågor som rör IT-säkerhet, MSB, <https://www.msb.se/contentassets/b0614486a8c04a198cb885b8b9df677b/slutrapport-it-sakerhet-2024.pdf>

National capabilities assesment framework 2020, ENISA, <https://www.enisa.europa.eu/sites/default/files/publications/WP2020%200.3.1.2%20National%20Capabilities%20Assessment%20Framework.pdf>

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

Sex förslag för en stärkt kompetensförsörjning inom informationssäkerhet;
Universitetskanslersämbetet, Tillväxtverket, Luleå tekniska universitet och MSB,
<https://www.myh.se/om-oss/myndighetssamverkan-och-samverkansprojekt/myndighetssamverkan/aktuellt-inom-myndighetssamverkan/sa-kan-kompetensforsorjningen-starkas-inom-cybersakerhet>

Svårlurad, Sveriges banker och Svenska Bankföreningen,
<https://svarlurad.se/>

Digitalidag, PTS,
<https://digitalidag.se/start>