Myndigheten för samhällsskydd och beredskap

FÖRSTUDIE

Kompetens inom informations- och cybersäkerhet

En förstudie om kompetensförsörjning för samhället

Kompetens inom informations- och cybersäkerhet - En förstudie om kompetensförsörjning för samhället

Text: Avdelningen för cybersäkerhet och säkra kommunikationer, enheten för systematisk informationssäkerhet

Innehåll

Kompetens inom informations- och cybersäkerhet

Denna förstudie redovisar möjligheter att stödja kompetensförsörjningen på informations- och cybersäkerhetsområdet i Sverige. Resultatet är ett antal förslag på åtgärder som krävs för att kunna säkerställa god kompetensförsörjning över tid och utifrån samhällets behov. I analysen har flera aktörer involverats.

Förstudien har till största del genomförts mellan september 2019 och juni 2020. Slutbearbetning har gjorts under 2021.

Bakgrund

Regeringens nationella strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213)[1] har som syfte att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt höja medvetenheten och kunskapen i hela samhället.
MSB har tillsammans med flera andra myndigheter tagit fram en handlingsplan, *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022*, med 77 åtgärder som hänvisar till de sex strategiska prioriteringarna i den nationella strategin.
En av de 77 åtgärderna är att genomföra denna förstudie:

> ***Genomföra en förstudie rörande kompetensförsörjning inom informations- och cybersäkerhetsområdet för samhället.***
> *MSB avser att analysera möjligheterna att stödja utvecklingen av kompetensförsörjning inom informations- och cybersäkerhetsområdet. MSB ska även lägga förslag på åtgärder i form av styrning och stöd som detta skulle förutsätta inom olika typer av utbildningar så som yrkesutbildningar, vidareutbildningar, högskola och gymnasium.*

Regeringen uttryckte 2017 att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter (dnr N2017:03643)[2]. I takt med en ökad digitalisering, nya vanor och den it-tekniska utvecklingen finns det ett starkt behov av att skydda både människor, information och infrastruktur.

Digitaliseringstakten är just nu hög i samhället och den ökar alltjämt. Den rådande bristen på tillgänglig kompetens som kan bidra i digitaliseringsinitiativen riskerar på sikt att leda till en generellt undermålig säkerhetsnivå.

[1] https://www.regeringen.se/rattsliga-dokument/skrivelse/2017/06/skr.-201617213/
[2] https://www.regeringen.se/informationsmaterial/2017/05/for-ett-hallbart-digitaliserat-sverige---en-digitaliseringsstrategi/

Förstudien föreslår ett antal åtgärder om syftar till att på kort och längre sikt komma till rätta med denna kompetensbrist för att kunna följa den nationella strategin. God kompetensförsörjning bör säkerställa resurser för de framtida behov som digitaliseringen skapar, bidra till ökad kunskap om förebyggande och hantering av såväl it-relaterade brott som informationssäkerhets- och personuppgiftsincidenter, samt skydd av de informationstillgångar som är skyddsvärda för samhällsviktiga verksamheter.

Mål och syfte

Förstudiens övergripande mål är att kartlägga nuläget och ta fram åtgärdsförslag i syfte att bidra till kompetensförsörjningen på informations- och cybersäkerhetsområdet i Sverige.

Omfattning och avgränsningar

Förstudien omfattar offentliga och privata organisationers tillgång till yrkesverksamma med kompetens på informations- och cybersäkerhetsområdet. Därmed inkluderar förstudien målgrupper som är eller kommer att vara yrkesverksamma på kortare och längre sikt.

Fler målgrupper i samhället behöver närliggande kunskaper. Relevanta exempel kan vara barn som i tidig ålder exponeras för digitala medier och äldre som behöver hantera nya digitala verktyg. Dessa målgrupper behöver öka sitt säkerhetsmedvetande och få kunskap om hur de kan skydda de uppgifter som är viktiga för dem i samband med nya levnadssätt och vanor. Denna förstudie kommer dock inte beröra vad medvetenhet inom informations- och cybersäkerhet kan ge för nyttoeffekter utan fokuserar på särskilda målgrupper som redovisas under avsnittet Målgrupper och behov.

Begreppsförklaringar

På informations- och cybersäkerhetsområdet finns det många begrepp som är internationella och som dessutom är nya och saknar definitioner. I arbete med olika intressentgrupper har det varit tydligt att olika intressenter definierar begreppet cybersäkerhet olika, vilket också innebär att kompetenser inom området definieras olika. Det finns ett flertal publicerade rapporter som har gjort olika tolkningar av relevanta begrepp och det kan konstateras att det i nuläget saknas gemensamma definitioner av begreppen informationssäkerhet, cybersäkerhet och it-säkerhet.

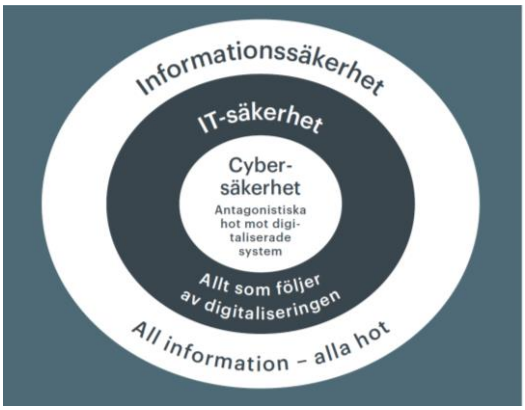
Denna förstudie utgår från den begreppsförklaring som återfinns i den nationella strategin för samhällets informations- och cybersäkerhet (se tabell nedan) och kommer inte vidare att definiera dessa begrepp. Begreppen informationssäkerhet och cybersäkerhet i strategin definieras i ljuset av den tidigare Säkerhetsskyddslagen (2018:585). I arbetet med att identifiera relevanta kompetensbehov görs i denna förstudie hålls dessa samman till ett enda säkerhetsområde.

Informationssäkerhet	Informationssäkerhet handlar om strävan att skydda information. Skyddet omfattas både av administrativa och tekniska åtgärder. Informationssäkerhet utgår från aspekterna om tillgänglighet, riktighet, konfidentialitet och spårbarhet.[3]
Cybersäkerhet	Cybersäkerhet innebär de mekanismer och åtgärder som används för att skydda cyberdomänen. Att skydda nätverkens och infrastrukturens tillgänglighet, integritet och konfidentialitet för den information som finns inom cyberdomänen. [4]

Det finns även andra närliggande begrepp som kan redovisas för att ge en helhetsbild över de kompetenser som behövs kopplat till informations- och cybersäkerhet.

It-säkerhet	Att skydda it-baserade informationssystem mot alla typer av företeelser så som intrång och avbrott.[5]
Digitalisering	Begreppet digitalisering innefattar främst kommunikaton och interaktioner mellan människor och verksamheter som sker via digitala verktyg/kanaler.[6]

Ovanstående begrepp går oftast inte att prata om som ett avskilda eller separata objekt. I rapporten *Digitalisering för ökad konkurrenskraft* [7] från Kungliga ingenjörsvetenskapsakademin beskrivs relationen mellan begreppen enligt denna bild i Figur 1.



Figur 1

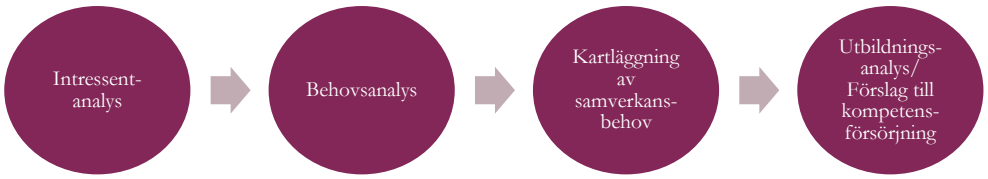
Termer inom informations- och cybersäkerhetsområdet kommer att definieras och göras allmänt tillgängliga genom MSB:s arbete med en nationell terminologi.

[3],[4] https://www.regeringen.se/49bb84/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523

[5] https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf
[6] https://digitaliseringsradet.se/sveriges-digitalisering/begrepp/
[7] https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf

Metod och genomförande

Underlaget i förstudien har delvis tagits fram genom olika intressent- och behovsanalyser. De behov som har identifierats har därefter undersökts vidare för att se vilka utbildningsinstanser som kan bidra till just de specifika kompetensförsörjningsbehoven. Genom workshops har flera arbetsgrupper involverats i att ta fram underlag för att kunna identifiera olika målgrupper och åtgärdsförslag.



Förstudiens undersökningsdelar har bestått av följande:

- Workshop för att identifiera intressenter inom både offentlig och privat sektor.
- Samverkan med intressenter för att ta fram en beskrivning av nuläge.
- Workshop med intressenter för att identifiera målgrupper och utbildningsnivåer.
- Kartläggning av befintliga utbildningar.
- Samverkan och samarbete med berörda externa aktörer för att ta fram förslag för kompetenshöjande åtgärder.
- Inhämta interna och externa behov för att vidare analysera resultatet och ta fram åtgärdsförslag.
- Samverkan med berörda aktörer för att vidare analysera åtgärdernas förutsättningar.

Kartläggningen av befintliga utbildningar undersökte vilka utbildningar (offentligt och privat) som fanns tillgängliga och som skulle kunna utgöra en del av kompetensförsörjningen inom området. Detta genomfördes under perioden oktober 2019 t.o.m. april 2020. Det har inte varit möjligt att säkerställa att listan på utbildningar är komplett. En förteckning över identifierade utbildningar under perioden återfinns i bilaga 1.

Intressenter

Aktörer som har deltagit och bidragit till underlag för analys:

Aktör	Analystyp
MSB	Intressentanalys och behovsanalys
KIS-nätverket (Kommuners informationssäkerhet)	Behovsanalys inom kommunalförvaltning

HoSiS-nätverket (Hälso- och Sjukvårds Informationssäkerhet)	Behovsanalys inom regionförvaltning
SOFF-nätverket (Säkerhets- och försvarsföretagen)	Behovsanalys inom näringslivet
SAMFI – samverkansgruppen för informationssäkerhet	Behovsanalys inom egna myndigheterna.
SNITS (MSB:s nätverk för statliga myndigheter)	Behovsanalys inom den offentliga sektorns förvaltning
Myndigheten för digital förvaltning Tillväxtverket och Universitetkanslerämbetet	Samverkan
Försvarshögskolan Universitetkanslerämbetet Myndighet för yrkeshögskola Högskolan i Skövde UR skola	Utbildningsanalys

Nuläge

Hur stor är kompetensbristen?

De nationella strategierna kopplade till digitalisering och informations- och cybersäkerhet driver på utvecklingen. Tillgång till kompetens på informations- och cybersäkerhetsområdet behövs i takt med att digitaliseringen ökar och de hotbilder, risker och sårbarheter som den för med sig förvärras. Digitaliseringen drivs framåt genom agila arbetssätt för att bättre kunna möta behoven som hela tiden förändras. De agila arbetssätten ställer höga krav på närvaro i utvecklingsarbetets alla steg. Nuvarande arbetssätt på informations- och cybersäkerhetsområdet stödjer inte alltid detta och nu tillgänglig kompetens räcker inte till för att delta i de agila arbetssätten utifrån nu givna förutsättningarna. Det behöver säkerställas att tillgången på kompetens inom området är tillräcklig för att motverka digitaliseringens negativa effekter.

Det saknas i nuläget möjlighet att kartlägg av omfattningen på kompetensbristen på informations- och cybersäkerhetsområdet i Sverige. Viss vägledning kan dock hämtas ur rapporter från IT- och telekomföretagen och SCB, samt från internationella undersökningar. Här följer en kort översikt över resultaten från de senaste undersökningarna.

IT-kompetensbristen, en rapport från IT- och telekomföretagen

IT- och telekomföretagen publicerade 2020 en rapport[8] där en uppskattning görs av att det år 2024 kommer att saknas 70 000 personer med kompetenser inom IT och digitalisering, samma antal som 2017 förutspåddes saknas 2022.

Rapporten fokuserar främst på it-kompetens och använder begrepp som data-/it-/informationssäkerhet. Bland drivkrafter som påverkar kompetensbehovet finns data-/it-/informationssäkerhet på tredje plats medan nya och ändrade regelverk kopplat till integritet och säkerhet hamnar på femte plats. It-/informationssäkerhet återfanns på samma lista också 2017.

Behovet av personer med it- eller informationssäkerhetskompetens bedöms öka med ca 900 personer på fyra års sikt. Dock konstateras att det officiella yrkesregistret (SSYK), som utgjort basen för beräkningarna, inte fångar in många av de kompetenser och roller som omfattas av kartläggningen vilket leder till en underskattning av behovet. Ett tydligt exempel lyfts fram: enligt yrkesregistret finns ca 2300 verksamma it-säkerhetsexperter idag, medan de drygt 200 bolag som svarat på enkäten (dvs inte ens hela branschen) uppger att de har närmare 4000 medarbetare med antingen it- eller informationssäkerhet som sin huvudsakliga kompetens idag.

På frågan vilken yrkeserfarenhet som efterfrågas svarar 44 % (informationssäkerhet) resp. 47 % (it-säkerhet) att personerna som behövs som regel behöver ha minst 5 års erfarenhet medan 50 % (informationssäkerhet) resp. 46 % (it-säkerhet) att personerna behöver ha mellan 3 och fyra års erfarenhet.

Motsvarande kartläggning för andra sektorer respektive offentlig sektor finns inte idag.

SCB:s arbetskraftsbarometer

SCB kategoriserar inte informations- eller cybersäkerhet separat men det kan antas att en stor del av blivande resurser inom området kan hämtas från dessa utbildningar, i synnerhet inom de mer tekniska inriktningarna. Det ska dock påpekas att många andra utbildningar också kan vara en inkörsport till informations- och cybersäkerhetsområdet, exempelvis juridik och samhällsvetenskap.

Barometern visade 2020[9] på en växande brist inom flera av de yrkeskategorier där informations- och cybersäkerhetskompetenser ofta jobbar.

- På gymnasienivå anger arbetsgivarna framförallt brist på yrkeserfarna med utbildning inom dator- och kommunikationsteknik. För nyutexaminerade är tillgången balanserad. Andel arbetsgivare som anger brist på yrkeserfarna har stigit från 40 % 2015 till 70 % idag.

[8] https://www.almega.se/app/uploads/sites/2/2020/12/ittelekomforetagen-it-kompetensbristen-2020-online-version.pdf
[9] https://www.scb.se/contentassets/03e7444790f54d6d94479e1ba76d7c6b/uf0505_2020a01_am78br2003.pdf

- Det är fortsatt stor brist på yrkeserfarna civilingenjörer inom elektronik, datateknik och automation. För nyutexaminerade är bilden mer varierad. 40 % anger brist på nyutexaminerade, 90 % brist på yrkeserfarna. Samtidigt rapporterar arbetsgivarna ökade anställningsbehov på sikt.

- Ungefär 8 av 10 arbetsgivare uppger brist på yrkeserfarna högskoleingenjörer inom el, elektroteknik och datateknik. För nyutexaminerade ger arbetsgivarna en mer varierad bild av tillgången.

- För universitetsutbildade bedömer arbetsgivarna att tillgången på nyutexaminerade programmerare och systemvetare är i balans. Arbetsgivarna uppger fortsatt brist på arbetssökande med yrkeserfarenhet.

The Life and Times of Cybersecurity Professionals 2021, by ESG and ISSA

Rapporten[10] är den femte i en serie som undersöker hur cybersäkerhetsprofessionen i världen lever och utvecklas. I rapporten konstateras att trots att diskussionen om kompetensbrist på området har pågått i över tio år har det inte skett några större framsteg mot en lösning under de fem år man har rapporterat på utvecklingen. Årets rapport bygger på en undersökning som har besvarats av 489 cybersäkerhetsexperter och visar bland annat att:

- Kompetensbristen har påverkat över hälften (57 %) av organisationerna.
- De största konsekvenserna av kompetensbristen är ökande arbetsbelastning (62 %), vakanta positioner som inte kan tillsättas (38 %) och utbrändhet (38 %).
- 95 % av respondenterna anger att kompetensbristen och dess konsekvenser inte har förbättrats under de senaste åren, medan 44 % anger att det dessutom har blivit värre.
- Personer med 4-7 års erfarenhet (41 %) och personer med 7+ års erfarenhet (30 %) är svårast att rekrytera.
- Medan 91 % av respondenterna anger att personer inom professionen löpande behöver utveckla sin kompetens för att kunna möta den ständigt föränderliga hotbilden anger 59 % att arbetsbelastningen inte medger sådan kompetensutveckling.

Sammanfattning

Bristen på kompetens inom informations- och cybersäkerhet är ett globalt problem och trenden i Sverige skiljer sig sannolikt inte avsevärt från den internationella utvecklingen. Ökande arbetsbelastning och risk för ohälsa, tillsammans med bristande möjligheter att löpande hålla sig uppdaterad med

[10] https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

förändringar riskerar att i förlängningen att ytterligare minska intresset för att arbeta med frågorna.

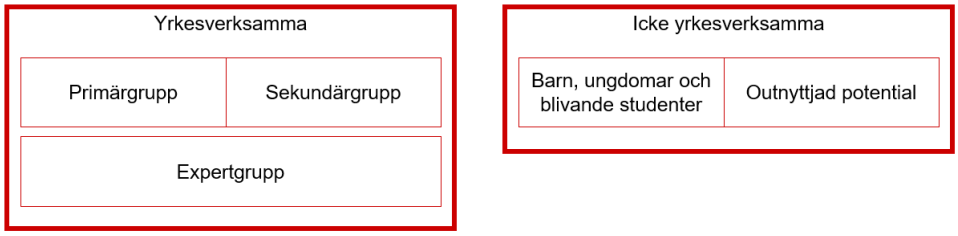
Efterfrågan på kompetenser med lång erfarenhet av arbete med informations- och cybersäkerhet är hög. Sådan kompetens kan enbart erhållas genom flera års arbete i relevanta positioner. Det är därför viktigt att både fylla på med nyutbildade och att stötta befintlig kompetens så att efterfrågan på erfarna personer kan mötas även i framtiden. Det kommer dock av naturliga skäl att ta tid att fullt ut möta behoven, det finns inga genvägar till den typ av erfarenhet som efterfrågas.

Målgrupper och behov

Det saknas idag en fullständig bild av samhällets generella kunskapsnivå inom information- och cybersäkerhet. Nyttoeffekterna av de kompetenshöjande åtgärder som föreslås kan därför inte kopplas direkt till kunskapsnivåer.

Roller och kompetenser inom informations- och cybersäkerhet är inte enhetligt definierade. Det finns inga specifika gymnasie- eller högskoleutbildningar med inriktning på dessa områden och heller inga definierade yrkestitlar vilket innebär att vem som helst kan kalla sig för exempelvis informationssäkerhetsspecialist.

Kompetens kan skaffas på två sätt, genom utbildning eller genom erfarenhet. I de flesta fall byggs kompetens på en kombination av utbildning och erfarenhet.
I denna förstudie delas den identifierade målgruppen in i två huvudgrupper. Figur 2 illustrerar de båda huvudgrupperna - de som idag är yrkesverksamma och de som ännu inte är yrkesverksamma. Nedan följer en översikt över dessa grupper och undergrupper.



Figur 2.

Yrkesverksamma på området

Den yrkesverksamma målgruppen kan delas upp i tre undergrupper. Primärgruppen är den grupp som idag arbetar inom informations- och cybersäkerhetsområdet. Sekundärgruppen består av yrkesverksamma i närliggande områden där förståelse för och kunskap om informations- och cybersäkerhet är viktigt. Expertgruppen består av personer som har tillskansat sig så mycket kunskap, erfarenhet och kompetens på informations- och cybersäkerhetsområdet att de kan bidra till andras lärande.

Primärgrupp

I primärgruppen finner vi idag ett stort antal personer som nyligen har fått arbetsuppgifter inom området, men som helt saknar utbildning på området. Denna grupp behöver utbildning på grundläggande nivå för att alls kunna börja utföra sitt jobb.

En stor andel av den primära gruppen består av personer som på olika sätt har ”halkat in” på området, ofta från närliggande roller (se sekundärgruppen). Dessa och andra som på olika sätt redan har tillskansat sig en grundläggande kompetens har behov av fördjupande utbildningsinsatser.

Redan idag och i ökande utsträckning behöver alla i primärgruppen löpande utbildning för att hålla sig uppdaterad med utvecklingen på området och det finns ett generellt behov att utveckla sig inom relaterade områden som metodanvändning, it-säkerhet, juridik och upphandling.

Primärgruppen behöver utbildnings- och inlärningsformer som är anpassade till yrkesverksamma. Med andra ord korta utbildningar som inte kräver avbrott från det ordinarie arbetet under någon längre tid, utbildningar som är subventionerade av arbetsgivaren och kan genomföras under arbetstid eller distansutbildningar som möjliggör flexibel studietakt.

Sekundärgrupp

I sekundärgruppen finns de yrkesverksamma som har huvudarbetsuppgifter som inte ligger inom informations- och cybersäkerhetsområdet. Här hittar vi roller som chefer, upphandlare, jurister med många fler. Trots att de inte arbetar med informations- och cybersäkerhet behöver de en grundförståelse för frågorna samt särskilda utbildningar som är anpassade för deras roller.

Likt primärgruppen behöver sekundärgruppen utbildnings- och inlärningsformer som är anpassade till yrkesverksamma.

För att kunna anpassa utbildningar behöver de olika yrkesrollerna i sekundärgruppen kartläggas och eventuellt olika behov hos olika roller identifieras.

Expertgrupp

I den yrkesverksamma målgruppen finns det också en undergrupp med experter. Idag är det väldigt få inom branschen som anses vara experter. På forskarnivå finns det ett antal inom data- och systemvetenskap i Sverige. När högskolor och universitet håller kurser som berör informations- och cybersäkerhet bjuds ofta externa resurser från näringslivet in.

Ett särskilt fokus behöver riktas till försörjning av experter som kan bidra till andras lärande. Med flera experter/utbildare kan kompetensförsörjningen bli cirkulär.

Icke yrkesverksamma på området

Den andra huvudgruppen *icke yrkesverksamma* har också två undergrupper. En grupp består främst av barn och ungdomar som är i skolan och inte är ute i

arbetslivet än. Den andra gruppen är de som har goda kunskaper inom informations- och cybersäkerhet eller närliggande områden, men som av olika skäl har valt att inte arbeta eller vidareutbilda sig inom området. Primärt ligger det i samhällets, snarare än gruppernas egna, intresse att här väcka engagemang i informations- och cybersäkerhetsfrågorna.

Barn, ungdomar och blivande studenter

För gruppen barn och ungdomar är användning av och tillgång till information, internet och sakernas internet en del av vardagen. Denna grupp behöver se informations- och cybersäkerhet som en lika självklar komponent i vardagen som allt digitalt och få tillräckligt mycket information om framtida utbildnings- och karriärmöjligheter för att se arbete inom området som ett intressant yrkesval.

Outnyttjad potential

Den kanske svåraste gruppen att nå är den som har goda kunskaper på informations- och cybersäkerhetsområdet, men som inte har ett intresse av att utbilda sig eller arbeta inom området. Här finns till exempel personer som har lämnat området eller som arbetar på närliggande områden, som it-utveckling och/eller -drift, juridik, arkiv med mycket mer som av olika skäl inte låter sig lockas att fördjupa sitt engagemang informations- och cybersäkerhetsområdet. Denna grupp har kanske varken en registrerad akademisk examen eller söker jobben inom informations- och cybersäkerhet. Den här gruppen behöver få ett intresse för området och mötas av mer kreativa rekryterings- och matchningsprocesser.

Sammanfattning

Bland de som är yrkesverksamma på området märks behov av att kunna kompetensutveckla sig och hålla sig uppdaterad på området parallellt med det dagliga arbetet. Kompetensnivån varierar kraftigt och det finns ett behov av att fylla på med både mer erfarna yrkesverksamma och experter som kan bidra till andras lärande.

Bland de som ännu inte är yrkesverksamma på området märks ett samhällsbehov av att skapa tydliga och lockande vägar till att bli yrkesverksam på området.

Detta innebär att det krävs en ganska bred satsning för att förbättra förutsättningarna för de redan yrkesverksamma på området att fördjupa och underhålla sin kompetens. Det krävs också någon form av standardisering av yrkestitlar och vägar till dessa för dem som ännu inte är yrkesverksamma.

Vägar till kompetens

De vägar som hittills har lett till kompetens på informations- och cybersäkerhetsområdet är disparata. I takt med att efterfrågan har växt har enskilda individer trampat upp sina egna stigar till kompetens på området. Gemensamt för många av dessa stigar är att de i första hand har handlat om att utgå ifrån ett eget intresse och själv söka information och kunskap om frågorna.

Parallellt med den utvecklingen har också utbudet av utbildningar ökat. Utbildningar som redovisas i denna förstudie kartlades oktober 2019 - februari 2020. Trots att nya utbildningar introduceras emellanåt krymper dock inte efterfrågan. En stor del av förklaringen till det är att efterfrågan i sig ökar, men en del av förklaringen ligger också i att efterfrågan inte begränsar sig till nyutbildade/juniorer – efterfrågan på seniorer, experter och specialister kan inte kortsiktigt påverkas genom utbildningsinsatser.

Digitaliseringstakten ställer också höga krav både på utbildningar och på yrkesverksamma att proaktivt hålla sig uppdaterade med utvecklingen för att kunna hantera ständigt nya typer av sårbarheter och hot.

Sammantaget kan konstateras att utbildningsvägar behövs för kompetensförsörjningen, särskilt på sikt, medan vägar för att underhålla, komplettera och vidareutveckla befintlig kompetens behövs för att också säkerställa mer senior kompetens. Nedan följer en översikt av det nuvarande utbudet av utbildningar och andra vägar till kompetens.

Utbildningar

Gymnasieutbildning

Det finns några gymnasieutbildningar med inriktning mot it i allmänhet men som också innehåller en hel del it-säkerhet, exempelvis på NTI-gymnasiet som finns på många orter. Som de allra flesta gymnasieutbildningar så är fokus främst på att erhålla högskolebehörighet snarare än en färdig yrkesutbildning.

Komvux

Kommunala vuxenutbildningen har som främsta syfte att ge personer, som saknar behörighet till högre utbildning, möjlighet att komplettera sina gymnasiebetyg. Några specifika utbildningar med inriktning på informations- och cybersäkerhet verkar därför inte finnas.

Yrkeshögskola

Yrkeshögskolorna har ett antal informations- och it-säkerhetsutbildningar som riktar sig till de som vill skaffa sig en yrkesutbildning med goda möjligheter till anställning. Utbildningarna är eftergymnasiala och omfattar ett till två års heltidsstudier. Yh-utbildningar kan ofta genomföras på distans och med lägre studietakt och passar därför väl som kompetenshöjande utbildning för redan anställda. Yh-utbildningar leder till yrkeshögskoleexamen eller kvalificerad yrkeshögskoleexamen.

Högskoleutbildning

I första hand för gruppen icke yrkesverksamma, men kan också vara aktuellt för den som vill förkovra sig och byta arbetsuppgifter. Det finns både breda utbildningar (civilingenjör, systemvetare) men också specifika it- och cybersäkerhetsutbildningar främst inom ramen för högskoleingenjörsutbildningar.

Vidareutbildningar och fördjupningsutbildningar för yrkesverksamma som grupp

Det finns ett flertal företag som erbjuder utbildningar i informations- och cybersäkerhet. Längden på utbildningarna är från en dag upp till några veckor. Kostnaden är vanligen ganska hög så det är främst anställda där arbetsgivaren sponsrar som är målgruppen.

Bilaga 1 listar exempel på sådana utbildningar.

Andra vägar

Certifieringar

Personcertifieringar med relevans för arbetsuppgifterna efterfrågas ibland som komplement till formell utbildning. De vanligaste certifieringarna inom detta område tillhandahålls av ISACA, exempelvis CISA (certified information systems auditor) och CISM (certified information security manager). En annan vanlig certifiering är CISSP (certified information systems security professional) som administreras av ISC (International Information System Security Certification Consortium). En fördel med dessa certifieringar är att de kräver ett löpande underhåll genom deltagande i kurser, seminarier eller relevanta arbetsuppgifter. Hur väl en certifiering faktiskt avspeglar individens kompetens är dock svårt att bedöma.

Kompetensutveckling i arbetet

Den vanligaste kompetensutvecklingen sker på arbetsplatsen i samverkan med andra. Det är viktigt att arbetsgivaren inser detta och stöttar arbetssätt som ger nyanställda möjlighet att lära av mer erfarna medarbetare. Det är också viktigt att medarbetare successivt får mer utmanande arbetsuppgifter utan att för den skull ställas helt utan stöd och uppbackning.

Nätverk, föreningar

Deltagande i intresseföreningar och nätverk kan bidra till en högre kompetens generellt, i synnerhet om dessa rör den specifika bransch eller verksamhet som personen verkar inom. Några exempel är Information Security Forum (global organisation med både offentliga och privata deltagare), SNITS (MSB:s nätverk för statliga myndigheter) och SIG-Security (förening för personer som arbetar professionellt inom området informations- och it-säkerhet).

Sammanfattning

Det finns idag många olika vägar till kompetens på området, men innehållet är spritt och det är svårt att fånga några tydliga mönster för hur till exempel vidareutveckling av egen kompetens kan genomföras för att fördjupa och uppdatera över tid eller hur utbildning med examination ska utformas.

Det går heller inte att idag utröna på vilket sätt, om alls i någon större utsträckning, informations- och cybersäkerhetsfrågor integreras i andra utbildningar. Detta gäller såväl grund- och gymnasieskola som högskoleutbildningar på andra, relaterade områden.

Slutsatser

För att säkra kompetensförsörjningen i Sverige krävs att samhället gör en målriktad satsning med flera parallella åtgärder. Insatser behöver vara av olika karaktär och på flera utbildningsnivåer samtidigt för att alls börja säkerställa tillgång till rätt kompetens på både kort och lång sikt.

Det krävs ett arbete för att förtydliga och definiera vilka typer av roller som finns på området samt säkerställa vilken typ av kompetens och kunskap som krävs för att kunna arbeta i dessa roller. Detta ger möjlighet att över tid följa kompetensförsörjningen och ge underlag för framtida insatser samt ett underlag för att skapa en eller flera röda trådar som kan leda från grundskolan och hela vägen genom en högskoleutbildning.

Det krävs också flera kartläggningsinsatser för att identifiera vilken typ av kompetens och kunskap som bör förmedlas genom utbildning av olika slag, vad som hindrar olika typer av utbildningsorgan från att tillhandahålla nödvändiga utbildningar och/eller vad som hindrar personer från att tillgodogöra sig befintliga utbildningar. Detta kan leda till standardiserade vägar till kompetens på området, att krav kan ställas på utbildningar av olika slag och hinder röjas ur vägen.

Särskild uppmärksamhet bör riktas till att förflytta fler personer in i expertroller, detta för att dels säkra kompetens som kan bidra till andras lärande och dels för att kunna nyttja till utveckling av metoder och arbetssätt.

I en tid av intensiv digitalisering har området blivit, och blir ständigt alltmer, eftersatt. Efterfrågan ökar och trots att spridda insatser görs lyckas inte samhället säkerställa tillgången på kompetens till de som behöver det. Konsekvenserna av en digitalisering som tillåts fortlöpa utan stöd av kompetens på informations- och cybersäkerhet är svåröverblickbara. Det som med säkerhet kan sägas är att tillit och säker digitalisering inte kan garanteras – övriga konsekvenser är helt beroende av vad samhället väljer att digitalisera.

Förslag på åtgärder och fortsatt arbete

Nedan presenteras ett antal förslag på åtgärder som kan bidra till en stärkt kompetensförsörjning på informations- och cybersäkerhetsområdet.
Flera av åtgärdsförslagen kan med fördel slås samman och drivas i samma uppdrag. Det är viktigt att säkerställa att samverkan sker mellan myndigheter vars ansvarsområde omfattar utbildnings- och kompetensförsörjningsfrågor respektive innehållsfrågor, det vill säga informations- och cybersäkerhet. Arbetet bör ledas av den myndighet som bedöms kunna bli ansvarig för vidare åtgärder utifrån uppdragets resultat. På så vis kan arbetet formas utifrån typen av uppdrag samtidigt som lärdomar från arbetet enkelt kan överföras till implementering.

Hänsyn bör tas till åtgärder som föreslås eller genomförs inom ramen för andra uppdrag, till exempel uppdrag att samverka kring kompetensförsörjningen av

digital spetskompetens,[11] uppdrag att utveckla en sammanhållen datainfrastruktur för kompetensförsörjning och livslångt lärande[12] och uppdrag till Försvarsmakten och Säkerhetspolisen om kompetensförsörjning inom säkerhetsskyddsområdet.[13]

1. Definiera roller och kompetenser

För att få en gemensam utgångspunkt i vilka kompetenser samhället ska försörjas med behöver dessa definieras.

Identifiera och definiera de roller som finns på och nära området samt koppla relevanta kompetens-, erfarenhets- och kunskapskrav till dessa roller. Undersök möjligheten att nyttja SeQF[14] för att klassificera och utforma kvalifikationer för att säkerställa deras tydlighet, överförbarhet och kvalitet. Målet bör vara att resultatet ska kunna publiceras och användas dels för uppföljning av utvecklingen av kompetensförsörjning och för att utforma andra åtgärder av olika slag enligt nedan.

2. Utred de agila arbetssättens påverkan på informations- och cybersäkerhetsarbetet och konsekvenserna för behovet av kompetensförsörjning

För att säkerställa ändamålsenligt stöd till moderna arbetssätt krävs insikter och kunskap om vilka arbetssätt och vilken kompetens som behövs för att effektivt kunna möta de krav på lättrörlighet som ställs.

Utred vilka nya arbetssätt som kan behövas på informations- och cybersäkerhetsområdet för att stötta agila arbetssätt för digitalisering. Utred också om nya roller och/eller specifika kompetenser krävs för att dessa arbetssätt ska kunna användas. Målet bör vara att resultatet ska kunna publiceras och användas dels för uppföljning av utvecklingen av kompetensförsörjning och för att utforma andra åtgärder av olika slag enligt nedan.

3. Kartlägg och följ upp samhällets behov av kompetensförsörjning

För att säkerställa kompetensförsörjning över tid krävs löpande insikter om nuvarande och kommande kompetensbehov.

Utgå ifrån resultat från åtgärd 1 och 2. Säkerställ ändamålsenlig metod, format och ansvarig samt implementera löpande uppföljning av samhällets kompetensbehov över tid. Uppföljningen ska vara uppdelad på offentlig och privat sektor och bör undersöka minst

[11] https://www.regeringen.se/regeringsuppdrag/2019/08/uppdrag-att-samverka-kring-kompetensforsorjningen-av-digital-spetskompetens/
[12] https://www.regeringen.se/regeringsuppdrag/2021/06/uppdrag-att-utveckla-en-sammanhallen-datainfrastruktur-for-kompetensforsorjning-och-livslangt-larande/
[13] https://www.regeringen.se/pressmeddelanden/2021/05/uppdrag-till-forsvarsmakten-och-sakerhetspolisen-om-kompetensforsorjning-inom-sakerhetsskyddsomradet/
[14] https://www.seqf.se/

- hur många yrkesaktiva som finns i respektive roll,
- hur stor efterfrågan beräknas vara på tre till fem års sikt,
- om det tillkommer roller och/eller krav på kompetens och kunskap,
- vad konsekvenserna av en fortsatt kompetensbrist bedöms vara.

4. Kartlägg högskole- och yrkeshögskoleutbildningar och föreslå möjligheter att definiera och komplettera

För att säkerställa ett löpande tillflöde till juniora roller krävs utbildningar som i sig själva leder till sådana roller.

Utgå ifrån resultatet från åtgärd 1 och 2. Kartlägg vilka högskole- och yrkeshögskoleutbildningar som möter kraven på kompetens och kunskap för juniora roller. Föreslå ett utbud utbildningar med förslag till standardiserat innehåll som bör ingå för att en utbildning ska kunna sägas leda till en viss roll som bedöms täcka kompetensbehovet av juniorer på sikt.

Utgå ifrån resultatet från åtgärd 3 och utred vilka eventuella hinder som står i vägen för tillgängliga utbildningsorgan att tillhandahålla nödvändiga utbildningar samt vad som eventuellt hindrar personer att tillgodogöra sig de utbildningar som finns tillgängliga. Föreslå åtgärder som kan underlätta för utbildningsorgan att tillhandahålla nödvändiga utbildningar samt för personer att tillgodogöra sig de utbildningar som finns tillgängliga.

5. Kartlägg närliggande områden och föreslå möjligheter att integrera

För att kunna fånga informations- och cybersäkerhetsfrågor inom närliggande områden behöver utbildningarna inom dessa områden kartläggas för att sedan kompletteras.

Utgå ifrån resultatet från åtgärd 1 på närliggande områden, kartlägg högskole- och yrkeshögskoleutbildningar på dessa områden och föreslå standardiserat innehåll som behöver tillföras.

6. Utred behov i grund- och gymnasieskola och föreslå möjligheter att integrera

För att motivera och engagera elever att vilja välja utbildningar som leder till juniora roller behöver informations- och cybersäkerhet integreras i grund- och gymnasieskolan.

Utgå ifrån resultatet från åtgärd 1 och 2 samt ifrån åtgärd. Identifiera vilken information som behöver tillföras i grund- och gymnasieskola och hur den bäst integreras. Överväg särskilt behovet/möjligheten att skapa inriktningar mot området i gymnasiet.

7. Utred möjligheten och föreslå lösning på att certifiera utbildningsorgan

För att säkerställa att personer som redan är yrkesverksamma på området har tillgång till utbildningar som fördjupar kompetensen och håller sig uppdaterade med förändringar på området kan det behövas någon form av kvalitetsstämpel på relevanta utbildningar.

Utgå ifrån resultatet från åtgärd 1 och 2 relaterat till mer seniora roller och utred möjligheten att införa en certifiering för utbildningsorgan som riktar in sig på fördjupning av kompetens och uppdatering på området. Föreslå en ändamålsenlig lösning på att certifiera utbildningsorgan och/eller specifika utbildningar. Förslaget ska minst innehålla:

- Vem som ska certifiera.
- Vem/vad som kan certifieras.
- Hur certifiering ska genomföras samt underhållas över tid.
- Hur certifieringsprocessen kan användas för att löpande anpassa utbildningsutbudet till förändringar i omvärlden.
- Vem eller vad som kan eller bör kunna certifieras.

8. Utred möjligheter och föreslå åtgärder för att främja rörlighet för ökad kompetens

Ett sätt att skapa nya möjligheter till kompetensutveckling i arbetet är genom att öka möjligheterna att på olika sätt göra praktik och utbyta personal mellan organisationer. Detta kan åstadkommas genom till exempel praktikplatser, växeltjänstgöring, inlån, rörlighet inom staten och andra liknande åtgärder.

Utred möjligheter och former för att organisationer åläggs ett ansvar eller ges incitament att främja rörlighet inom informations- och cybersäkerhetsområdet genom att

- tillhandahålla möjligheter att för externa personer att delta i deras informations- och cybersäkerhetsarbete samt
- omvänt att bereda anställda möjlighet att delta i motsvarande arbete i andra organisationer.

Utred också specifikt offentlig sektors möjligheter att på ovanstående sätt främja rörlighet inom informations- och cybersäkerhetsområdet.

Beskriv förutsättningar och föreslå åtgärder som bedöms till ökade möjligheter till kompetensutveckling i arbete.

Bilaga 1 – Exempel på utbildningar inom informations- och cybersäkerhet

Denna översikt av befintliga utbildningar visar utbildningar (offentligt och privat) som fanns tillgängliga och som skulle kunna utgöra en del av kompetensförsörjningen inom området. Översikten sammanställdes under perioden oktober 2019 t.o.m. april 2020. Det har inte varit möjligt att säkerställa att listan på utbildningar är komplett.

Utbildningar som erbjuds av näringslivet

Lärosäte	Namn på utbildning	Studielängd
Dataföreningen	Strategisk informationssäkerhet	3-dagar
Dataföreningen	Operativ infomationssäkerhet	3-dagar
Dataföreningen	Teknisk informationssäkerhet	3-dagar
Dataföreningen	Certifierad informationssäkerhetsarkitekt	3-dagar
Dataföreningen	Teknisk informationssäkerhet	N/A
Xtractor	Inormationssäkerhet	Interaktiv
Sentor	Ciso as a service	N/A
Sentor	ISO 27000	N/A
Certezza	Grundläggande Utbildning I cert. mot ISO 27000	N/A
Certezza	Informations- och it-säkerhetsutbildning	N/A
Institut för juridisk utbildning	Infomrationssäkerhet	1 dag
Institut för informationsteknologi	Grundutbildning informationssäkerhet	3 dagar
Institut för informationsteknologi	It- och cybersäkerhet	2 dagar
DNV GL	ISO 27001 – Informationssäkerhet	1 dag
Oscarson Security AB	Grundkurs informationssäkerhet	1 dag
Oscarson Security AB	Systematiskt informationssäkerhetsarbete	1 dag
Draftit AB	Informationssäkerhet – Grundkurs	Distans

Canea	Grundkurs infroamtionssäkerhet och ISO 27001	1 dag
Canea	Ledningssystem för informationssäkereht i praktiken	2 dagar
Utbildning.se (del av Educations Media Group AB)	Informationssäkerhet i offentlig sektor	1 dag
Svenska Försäkringsföreningen	GDPR och informationssäkerhet	1 dag
Diploma utbildning	It- och informationssäkerhet	3 timmar
Fakultetskurser	Informationssäkerhet och sekretess ur legalt och praktiskt perspektiv	6 timmar
Svenska Försäkringsföreningen	GDPR och informationssäkerhet	Halvdag
Adding Value Consulting AB	CISM – Certified Inforamtion Security Manager	Distans
Adding Value Consulting AB	ISO/IEC 27001 Foudnation	Distans
Adding Value Consultning AB	ISO/IEC 27001 Foudnation – eLearning & Online-certifiering	Distans
SSF Stöldskyddsförening	Cybersäkerhet Utbildning Bas	1 dag
Diploma utbildning	It- och informationssäkerhet	2h 20 min – Distans
Bereau Veritas	Grundkurs ISO 27001	2 dagar
IFU	Cyber Risk Management	N/A
Learningtree	NIST Compliance Checklist training	1 dag
Learningtree	Cyber Security Training for managers and the boardroom	1 dag
Learningtree	Comp TIA Security	5 dagar
Learningtree	Certified Authorisation Professional	5 dagar
Learningtree	Certified Ethical Hacker	5 dagar
Learningtree	Certified Network Defender	On demand
Learningtree	Certifified Information Security Manager (CISM)	4 dagar
Learningtree	Certified Risk and information systems control (CRISC)	4 dagar
Learningtree	Certified Information systems auditor (CISA)	4 dagar
Learningtree	Comp TIA Cybersecurity Analys (CySA)	5 dagar

Securess	Cybersäkerhet Informationssäkerhet GDPR	N/A

Närliggande utbildningar

Företagsuniversitet	Informationssäkerhet för arkivarier	2 dagar
Institutet för juridiskgar utbildning	Patientdatalagen och informatiosnsäkerhet	6 timmar
Canea	Interrevision ISO 27001	1 dag
SSF Stöldskyddsföreningen	Säkerhetsskydd - introduktion	1 dag
Företagsuniversitet	Säkerhetschef 2030	8 dagar
Företagsuniversitet	Säkerhetssamordnare	9 dagar
IT Säkerhetsboalget	Hantera it-incidenter enligt NIS-direktivet	4 timmar
Fia Ewald Consulting AB	Praktisk informationssäkerhet	2 dagar
TechLaw	GDPR – Informationssäkerhet	Distans
VeaLearn	It- och informationssäkerhet – diplomerad onlineutbildning	2,5 timme
ATEA	Utbildning inom informationssäkerhet och GDPR	N/A
Diploma utbildning	It-säkerhet Grundkurs för anställda	45 min
Edument	Webbsäkerhet för utvecklare	2 dagar
Informator	Nätverksteknik och Datakommunikation	3 dagar
Informator	Webbsäkerhet – Attacker, Brandväggar, Kryptering	5 dagar
Informator	Secure web development and hacking for developers	3 dagar

Utbildningar som erbjuds av offentlig sektor

Lärosäte	Namn på utbildning	Studielängd
Försvarshögskolan	Chief information Assurance Officer	2 veckor

Försvarshögskolan	Inforamtionssäkerhet för chefer	1 dag
Stockholms universitet	Masterprogram i informationssäkerhet	2 år – 120hp
Karlstads Universitet	Högskoleingenjörsprogram i Datateknik	3 år -180hp
Malmö Universitet		
Högskolan i Skövde	Introduktion till Cybersäkerhet G1N	3 mån – 15 hp
Högskolan i Halmstad	It-forensik och informationssäkerhet	3 år
Luleå tekniska universitet	Informationssäkerhet, master	2 år – 120hl
Luleå tekniska universitet	Informationssäkerhet	3 veckor - 7,5hp
Örebros universitet		
FOI	Påbyggnadskurs i säkerhet i industriella informations- och styrsysten	3 dagar
Målardalens högskola	Praktiskt Cybersäkerhet	
MSB	DISA	Distans

Yrkeshögskoleutbildningar med aktörer från offentlig sektor och näringslivet

Lärosäte	Namn på utbildning	Utbildningslängd
Svensk institut för standarder	Grunderna i informationssäkerhet – steg 1 enligt ISO 27000	3 dagar
Svensk institut för standarder	Grunderna i informationssäkerhet – steg 2 enligt ISO 27000	3 dagar
Svensk institut för standarder	Att införa ett ledningssystem för informationssäkerhet	3 dagar
Svensk institut för standarder	Att leda och ständigt förbättra	3 dagar
Företagsuniversitet	Cybersäkerhet	10 veckor – 15 yh

Bildtext

Citat med linje

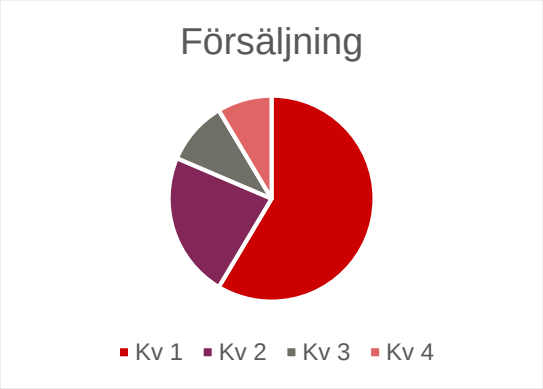
> **Faktaruta rubrik här**
>
> Faktaruta text här
>
> - Punktlista

Tabell 1. Rubrik till tabellen

Belopp anges i tkr	2017	2018	2019
Lorem ipsum	1 234	5 678	9 012
Lorem ipsum	1 234	5 678	9 012
Lorem ipsum	1 234	5 678	9 012
Lorem ipsum	1 234	5 678	9 012
Summa	**4 096**	**22 712**	**36 048**

Källa: Källa här

Figur 1. Rubrik till figuren



Källa: Källa här

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSBxxxxx - månad år ISBN ISBN