SÄKER DIGITALISERING HOS SMF

Kartläggning av små och medelstora företags behov och stödsystem i arbetet med informations- och cybersäkerhet

RAPPORTEN BESTÄLLD AV

tillväxt verket

Förord

Sverige är ett av EU:s mest digitaliserade länder, och har i sin digitaliseringsstrategi målet att vara bäst i världen på att använda digitaliseringens möjligheter[1]. Med hjälp av exempelvis AI och datadriven innovation kan verksamheter effektiviseras och nya produkter och tjänster skapas. Samtidigt medför en ökad digitalisering också risker, vilka i sin tur behöver värderas och hanteras för att säkerställa en hållbar digital utveckling.

Runt om i Sverige pågår flera satsningar på att öka digitaliseringen av samhället, men informations- och cybersäkerhet är sällan av första prioritet. För små och medelstora företag (SMF), som utgör majoriteten av företag i Sverige[2], kan arbetet med just informations- och cybersäkerhet vara en utmaning.

Syftet med rapporten är att kartlägga SMF:s stödsystem för en säker digitalisering samt identifiera SMF:s nuvarande och kommande behov av stöd i arbetet med informations- och cybersäkerhet. Kartläggningen består av tre huvudområden - kartläggning av initiativ och program, kartläggning av efterfrågan, samt sammanställning av rapporter. Målsättningen är att presentera rekommendationer kring vilka insatser som behövs samt vilka aktörer som är ansvariga för dessa insatser. Rapporten är framtagen av Unitalent AB tillsammans med Linköping Science Park och Blue Science Park, på uppdrag av Tillväxtverket inom ramen för regeringsuppdraget ”Höjd digital kompetens i småföretags ledningar och styrelser”. Slutsatser och förslag på framtida insatser är framtagna och skrivna av Daniel Kullgard och Lena Miranda på Linköping Science Park, medan resterande arbete av rapporten har genomförts av Elias Englund Forsblom, Estelle Lohm, Niklas Andersson och Sofia Ehn. Förhoppningen är att rapporten underlättar arbetet med hur SMF kan stöttas så de genomgår en säker digital transformation.

[1] Näringsdepartementet. 2017. *Ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*. Artikelnr: N2017.23. Regeringskansliet.

[2] Tillväxtverket. 2021. *Små och medelstora företags digitalisering – Vad har betydelse?* ISBN: 978-91-89255-10-4. Rapport 0366. Stockholm.

Sammanfattning

Digitalisering och säkerhet

Sverige ligger i topp vid flera internationella index vad gäller digitalisering, och är även ledande inom användning och investering i ny teknik. Däremot är landets små och medelstora företag, SMF, mycket mindre digitaliserade än de stora företagen. Digitaliseringen av dessa företag är viktig då det spelar stor roll för företagens lönsamhet, produktivitet och tillväxt. Med digitalisering kommer även en ökad sårbarhet där företag ofta är mål för cyberattacker. Bristande kompetens inom informations- och cybersäkerhet riskerar att skada företagen, bland annat genom försämrade kundrelationer, försämrat varumärke och större risk för attacker.

Rapportens syfte och avgränsningar

Syftet med rapporten är att kartlägga SMF:s stödsystem för en säker digitalisering samt identifiera SMF:s nuvarande och kommande behov av stöd i arbetet med informations- och cybersäkerhet. I rapporten ges rekommendationer kring vilka insatser som behövs. Avgränsningar har gjorts och rapporten behandlar enbart efterfrågan som finns hos SMF i Sverige, med fokus på SMF-techföretag och SMF som har en egen produkt- eller tjänsteutveckling. Arbetet har bestått av semi-strukturerade intervjuer och en litteraturstudie, där de intervjuade har representerat företagsfrämjare, branschorganisationer och företag. Även om intervjustudien har en relativ bredd med flertalet aktörer inom de olika kategorierna är urvalet väldigt litet i förhållande till målpopulationen. Det har gjorts en internationell utblick i rapporten, men den behandlar främst nationella stödsystem.

Litteraturstudiens resultat

Det har i litteraturstudien framgått att 80 % av svenska bolag har varit utsatta för minst en informationssäkerhetsincident under föregående år, och att det trots denna höga andel, även finns ett stort mörkertal bland utsatta. Under denna pågående pandemi har det även tillkommit nya och förändrade hot för företagen. Bland företag inom handeln förekommer kunskapsbrister vad gäller grundläggande säkerhetsfrågor och säkerhetsrutiner. Det finns bland dessa bolag även ett behov av att avstigmatisera utsattheten, så att personal vågar prata om kunskapsbristerna och företag vågar ta upp om man blivit utsatt. Bland småföretag inom jordbruk finns ett behov av att snabbt få hjälp om en IT-incident har skett, och en utmaning bland företagen är att se nyttan av de stora investeringar som krävs för att digitalisera en verksamhet, samt se nyttan för den kostnad säkerhetslösningar för med sig. I litteraturstudien framgick även att små tillväxtbolag har svårt att inse vad de kan vinna på kompetensutveckling och utbildning inom cybersäkerhet, något som också lyfts i flertalet intervjuer med branschorganisationer och företagsfrämjare. I dessa intervjuer lyftes att det upplevdes en ovilja hos de små tillväxtbolagen att lägga ner tid och pengar på de utbildningar som finns i dagsläget.

Behov hos tech-företag

I intervjuer med tech-företag nämndes att det fanns ett behov av fortsatt arbete med att utveckla kompetensen hos alla medarbetare på ett företag, för att minimera risken med att en ovetande medarbetare omedvetet skadar företaget. Det lyftes även ett behov av kunskap på en mer avancerad nivå, riktat till tech-företag, som idag har en högre IT-mognad än vad branschorganisationer och företagsfrämjare som erbjuder kurser inom cybersäkerhet besitter.

Produkt- eller tjänsteutvecklande företags behov

Hos produkt- eller tjänsteutvecklande företag är det inte lika hög IT-mognad som hos tech-företagen, vilket avspeglades i behoven som nämndes under intervjuerna med dessa företag. Det finns ett behov av grundläggande förståelse kring vad cybersäkerhet är och varför det är viktigt. Det framgick också att det kan vara svårt för företag som inte har egen IT-kompetens att ställa rätt krav på IT-leverantörer, och förstå hur säkra dess tjänster eller produkter är. I intervjuerna lyftes även en efterfrågan på utbildningar eller program som sträcker sig över en längre tid, anpassat efter företag, för att lättare etablera rutiner kring det företagsspecifika säkerhetsarbetet.

Kartläggning av utbudet till SMF

Kartläggningen som gjordes av utbudet riktat mot SMF är inte komplett, då relevanta delar kan saknas, och inkluderar bara den del av utbudet som tydligt riktar sig mot SMF alternativt en större målgrupp som SMF är en del av. Kartläggningen gör det dock tydligt att det finns stöd till SMF inom informations- och cybersäkerhet. Det finns utbildningar från flera offentliga aktörer, men även från några privata aktörer. Ett flertal privata aktörer erbjuder olika typer av försäkringar, och det finns även olika typer av konsulttjänster inom informations- och cybersäkerhet. Ett fåtal aktörer erbjuder olika typer av mindre tester och både privata och offentliga aktörer erbjuder informationsblad, guider, rekommendationer och checklistor. Vid mer passiva hjälpmedel, så som guider och tester, krävs att företagen själva letar upp informationen. En del av det utbud som hittades i kartläggningen riktar sig som nämnt till en större målgrupp, vilket gör att utbudet inte är specifikt utformat för SMF.

Rapportens slutsatser

Med ett ökat antal intrång och attacker i Sverige och globalt, finns en risk att företag och verksamheter avstår digitalisering, på grund av alla potentiella hot som digitaliseringen medför. Detta kan i sin tur bidra till minskad tillväxt och minskad innovation, vilket på längre sikt kan hämma Sveriges tillväxt. Frågan om säker digitalisering bör i stället lyftas proaktivt så att säkerheten integreras i den digitala utvecklingen från start.

Kompetens inom informations- och cybersäkerhet finns i Sverige, men den når inte ut till företagen. I dagsläget finns det många nationella initiativ, som står långt ifrån målgruppen SMF. Gränssnitten, som har bra kontakt med både akademi och näringsliv, finansieras inte i dagsläget, vilket gör att kunskapen har svårt att nå ut till företagen och paketeras efter deras behov. Det behöver därför riktas finansiering till gränssnitten, som har ett brett kontaktnät till både akademi och samhälle, och därmed har en viktig roll att spela.

Det är många frågor som konkurrerar om vikten på ett SMF:s strategiska agenda, bland annat hållbarhet, kompetensförsörjning och jämställdhet. Säkerhet har svårt att ta sig in på styrelse- och ledningsnivå i de små bolagen, som förväntas fokusera på många frågor vid sidan av kärnverksamheten och har svårt att få såväl ekonomiska som personella resurser att räcka till. Det kan även vara problematiskt att paketera ett budskap inom informations- och cybersäkerhet som riktas till en bred målgrupp. Förutsättningarna varierar mellan branscher, och även mellan företag inom branscherna.

Det visade sig även i intervjuer att företag som är leverantörer av IT-tjänster, förväntar sig att deras respektive leverantörer är säkra, vilket gör att frågan inte hanteras i den utsträckning som möjligtvis krävs. Det ligger ett stort ansvar på tjänsteleverantörer av IT-lösningar, då även de inom denna bransch utgår ifrån att sin leverantör levererar säkert.

Förslag på framtida insatser

Stödet till SMF bör finnas på olika nivåer och möta gruppens behov både kortsiktigt och på längre sikt. I rapporten framhävs ett behov av en nationellt ansvarig aktör, som har en samordningsfunktion med koll på vilken kompetens som finns hos olika myndigheter, lärosäten och forskningsinstitut samt privata aktörer. Det behövs en lärandeprocess mellan aktörer, där såväl samhällsskydd som näringsliv tas i beaktande. Den nationellt ansvarige skulle kunna vara ansvarig för informationsspridning inom informations- och cybersäkerhet riktat mot SMF.

Det behövs även en regional spridning av kunskap och tjänster, där det löpande kan genomföras utbildningsinsatser och information riktat till företagsfrämjare i ett kunskapshöjande syfte. Genom att utbilda företagsfrämjare når kunskapen ut till SMF i större utsträckning. En utgångspunkt för uppbyggnad av dessa regionala kontaktpunkter bör vara att förstärka och nyttja existerande strukturer. Denna regionala spridning kan även ske inom branscher och industrivertikaler, där de stora bolagen skulle kunna ta ett större ansvar att hjälpa sina underleverantörer, för att själva undvika attacker.

En help-desk dit företag kan vända sig om de blivit utsatta för en attack, skulle hjälpa företag att snabbare komma på fötter. Denna help-desk skulle även kunna svara på diverse frågor rörande informations- och cybersäkerhet och underlätta för företag som inte har egen IT-kompetens. Tanken är att stället kan erbjuda en tjänst där man kontaktar dem, likt 112, vid händelse av en attack eller generella frågor.

Ett annat förslag på framtida insatser är olika kompetenshöjande åtgärder. Dessa kan bestå av breddutbildningar som riktar sig till många, exempelvis styrelser och ledningsgrupper, samt integrerade utbildningsinsatser där det jobbas med pilotinsatser. Kunskapshöjande åtgärder kan också vara riktade utbildningar som är anpassade till företag och bransch, och som gärna ges under en längre tidsperiod. För att få företag att börja jobba med denna typ av insatser skulle det möjligtvis hjälpa med olika incitament, som exempelvis bidragsgivande kurser och kurser som ger högskolepoäng. Marknaden skulle även kunna ta fram olika utbildningar riktade till SMF, där framtagandet av utbildning bekostas offentligt, medan företagen själva får möjlighet att sälja utbildningen.

Innehåll

Bilagor

1 Inledning

I många internationella index för digitalisering placeras Sverige i en topposition[3]. År 2020 blev landet världsetta i Network Readiness Index (NRI)[4] och hamnade på en andra plats i EU-kommissionens Digital Economy and Society Index (DESI)[5]. Sverige nämns bland annat som ledande inom användning och investering i ny teknik[4], och ligger särskilt bra till när det gäller förutsättningar för digitalisering[5]. Däremot håller landets utveckling på att sakta in, och små och medelstora företag, SMF, är mycket mindre digitaliserade än de stora företagen[6].

99,9 procent av de cirka 1,2 miljoner företag som finns i Sverige idag är SMF[7]. De spelar en viktig roll för främjandet av konkurrenskraft och sysselsättning. Digitalisering av SMF är viktig då företag som utnyttjar digitaliseringens möjligheter presterar bättre än de företag som inte gör det till följd av kopplingen mellan digitalisering och produktivitet, lönsamhet, och tillväxt[2]. Men digitalisering av SMF innebär även ökad sårbarhet. Företag är ofta mål för allvarliga cyberattacker där exempelvis system stängs ned, känslig data läcks ut, eller elektroniska filer krypteras och lösensumma behöver betalas för att krypteringen ska hävas. Bristande kompetens inom informations- och cybersäkerhet riskerar skada kundrelationer, minska förtroendet för varumärket och bli en barriär för tillväxt.

Säkerhet har därmed blivit en affärskritisk fråga, och det är därför intressant att studera vilket stöd SMF har för att hantera digitala säkerhetsaspekter.

1.1 Syfte och målsättning

Syftet med rapporten är att kartlägga SMF:s stödsystem för en säker digitalisering samt identifiera SMF:s nuvarande och kommande behov av stöd i arbetet med informations- och cybersäkerhet. Kartläggningen består av tre huvudområden - kartläggning av initiativ och program, kartläggning av efterfrågan, samt sammanställning av rapporter. Målsättningen är att presentera rekommendationer kring vilka insatser som behövs samt vilka aktörer som är ansvariga för dessa insatser.

1.2 Avgränsning

Rapporten behandlar enbart efterfrågan som finns hos små och medelstora företag i Sverige. I Sverige tillämpas Europeiska kommissionens definition av SMF, vilket innebär att kartläggningen inkluderar företag som sysselsätter färre än 250 personer och har en årsomsättning som inte överstiger 50 miljoner euro eller en balansomslutning som inte överstiger 43 miljoner euro[8]. Vidare ligger fokus på SMF-techföretag samt SMF med egen produkt- eller tjänsteutveckling. Rapporten behandlar främst de nationella stödsystemen, men en internationell utblick har också genomförts.

---

[3] Digitaliseringsrådet. U.å. *Sveriges digitalisering*. https://digitaliseringsradet.se/sveriges-digitalisering/

[4] Dutta, S. Lanvin, B. 2020. *The Network Readiness Index 2020*. Portulans Institute. ISBN: 978-1-63649-055-7

[5] European Commission. 2020. *Digital Economy and Society Index (DESI) 2020*.

[6] DIGG. 2020. *Sverige på andra plats i EU-kommissionens mätning*. https://www.digg.se/om-oss/nyheter/2020/sverige-pa-andra-plats-i-eu-kommissionens-matning

[7] Tillväxtverket. 2021. *Basfakta om företag*. https://tillvaxtverket.se/statistik/foretagande/basfakta-om-foretag.html

[8] Europeiska unionen. 2015. *Användarhandledning om definitionen av SMF-företag*. Luxemburg: Europeiska unionens publikationsbyrå. ISBN 978-92-79-45300-7 doi:10.2873/94613

2 Bakgrund

Allt fler verksamheter digitaliserar hela eller delar av sin verksamhet[9]. Samtidigt blir cyberattacker allt vanligare och mer sofistikerade. För att säkerställa att verksamheter inte drabbas av dessa attacker är det viktigt med ett systematiskt säkerhetsarbete som genomsyrar hela organisationen. För att lyckas med detta är det viktigt att förstå vad informations- och cybersäkerhet innebär samt omfattningen av den digitala hotbilden mot företag.

2.1 Informations- och cybersäkerhet

I ett alltmer digitaliserat Sverige blir informations- och cybersäkerhet mer och mer aktuellt, samtidigt som begreppen kan vara svårtolkade. Informationssäkerhet innebär att skydda värdefull information utifrån krav på tillgänglighet, riktighet och konfidentialitet[10]. Med andra ord så ska information alltid finnas när vi behöver den, informationen ska vara korrekt, och endast behöriga personer får ta del av informationen. Cybersäkerhet kan kort beskrivas som ett samlingsbegrepp för de verktyg, metoder, teknik och teorier som individer och organisationer använder för att skydda system, nätverk, program, enheter och data från cyberattacker[11]. Skyddet riktar sig mot antagonistiska hot, till skillnad från IT-säkerhet som omfattar skydd av system mot företeelser som exempelvis felbedömningar och handhavandefel[12]. Till följd av ökat antal cyberattacker har behovet av kompetens inom informations- och cybersäkerhet ökat. Företag måste numera förstå hur de kan förebygga, upptäcka och hantera cyberattacker. Några av utmaningarna är att digitala intrång inte alltid är direkt synliga som fysiska intrång är, medvetenheten hos de anställda kan vara låg, och det krävs resurser för att exempelvis installera skyddssystem[13].

2.2 Lägesbild av de digitala hoten mot företag

De digitala hoten mot företag är mångfacetterade och förekommer på olika nivåer. Företag måste numera förebygga och hantera alltifrån överbelastningsattacker, dataintrång, cyberspionage och utpressning från enskilda hackers till statsunderstödda hacktivister. Utbud av exempelvis konsulthjälp inom informations- och cybersäkerhet finns men få erbjudanden är anpassade för SMF[18]. Många företag saknar även ekonomiska och personella resurser för att kunna möta säkerhetsutmaningarna digitalisering för med sig[14]. Exakta omfattningen av cyberattacker mot svenska företag är svår att överskåda då drabbade företag ofta håller det hemligt för att inte företaget ska förlora anseende[15].

I Tillväxtverkets rapport om informationssäkerhet publicerad hösten 2020 presenteras siffror för att illustrera den digitala hotbilden. Det finns 17 000 datorer och 400 000 mobila enheter med virus eller skadliga program, och 50 procent av Sveriges företag saknar

---

[9] FRA, Försvarsmakten, MSB, Polismyndigheten, Säkerhetspolisen. 2020. *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden*.

[10] MSB. 2019. *Informationssäkerhet i samhället*.

[11] IT Governance. U.å. *What is cyber security? Definition and best practices.* https://www.itgovernance.co.uk/what-is-cybersecurity

[12] Digitaliseringsrådet. 2020. *Rådet reflekterar – Risk i en digital tid*

[13] IT-finans. 2020. *Brister i cybersäkerhet kan betyda konkurs för mindre företag*. IT Media Group AB. https://it-finans.se/brister-i-cybersakerhet-kan-betyda-konkurs-for-mindre-foretag/

[14] Svenskt näringsliv. 2021. *Företagen och IT-säkerheten – hotbilder, motåtgärder och behov*

[15] Airaksinen, K. 2021. *Svenska företag döljer att de utsätts för cyberattacker*. SVT Nyheter https://www.svt.se/nyheter/inrikes/cyberattacker-med-utpressning-okar-kraftigt-mot-svenska-foretag

resurser för att klara en attack[16]. Det nämns vidare att de största cyberhoten mot svenska företag är den omedvetna medarbetaren, organiserad brottslighet och hacktivister.

En undersökning utförd av PwC våren 2020, baserad på 100 större företag, konstaterade att allt fler svenska bolag drabbas av cyberattacker[17]. 63 procent av bolagen uppger att de varit utsatta för minst en cyberattack under 2019 vilket är en ökning med 30 procent jämfört med 2018. Enbart 22 procent av de drabbade bolagen kan ange kostnaden för cyberattackshanteringen. Vidare uppges att användningen av molntjänster av företag förväntas öka vilket medför ökad risk för tredjepartsrisker som uppkommer i samband med outsourcing. En oroväckande trend som redovisas är att andelen informationssäkerhetschefer som rapporterar direkt till VD eller styrelse minskat från 28 procent till 14 procent. Få bolag ser alltså cybersäkerhet som en del i riskhanteringen i lednings- och styrelsearbetet. En kartläggning utförd av Tillväxtverket 2020 om digitala affärsrisker anger att kompetensen inom informationssäkerhet i ledning och styrelse är låg, men att medvetenheten kring cybersäkerhetsfrågor ökar[18]. Dock ökar medvetenheten främst i större företag.

Inom ramen för det nationella cybersäkerhetscentret publicerades 2021 en rapport angående cybersäkerhet i pandemitider, där redovisas bland annat hur svenska verksamheter i stort agerade. Det nämns att företagens exponering för cyberangrepp ökade under pandemin då arbetsplatsen förflyttades till hemmet[19]. Känslig information kommunicerades i digitala tjänster i stället för på kontoret, privat utrustning som inte uppfyllde säkerhetskrav användes i arbetssyfte, och tjänsteutrustning användes för privat bruk på ett sätt som exponerade den för angrepp. Samtidigt nämner rapporten att en del företag lättare kunde implementera nya tjänster med god säkerhet då de redan genomfört informationsklassningar av företagets informationstillgångar. Dessa företag kunde då lättare identifiera krypteringskrav, användarbehörighetskrav, och behov av autentisering. Generellt hanterade många cybersäkerhetsutmaningarna under pandemin väl, men det finns risk att incidenter som inträffat under pandemin ännu inte upptäckts.

2.3 Målgrupper

Kartläggningens målgrupper är SMF-techföretag samt SMF med egen utveckling. Övriga småföretag inkluderas också i rapporten för att kunna dra generella slutsatser om SMF efterfrågan av stöd på olika nivåer, både kortsiktigt och på längre sikt, sett till dagsläge och framtid. SMF delades in i tre kategorier, där den första kategorin *tech-företag* utgörs av SMF verksamma i techbranschen som har både nationella och internationella kunder. I kategorin *produkt- eller tjänsteutvecklande företag* ingår SMF som har egen produkt- eller tjänsteutveckling av något slag. I kategorin *övriga företag* ingår SMF som inte passade in i de andra två kategorierna. Den valda målgruppen grundar sig i att samhället präglas av komplexa digitala leveranskedjor där småföretagens brister inom IT-säkerhet riskerar drabba både dem själva, övriga organisationer, samt samhället i stort.

---

[16] Burvall, M. 2020. *Informationssäkerhet – Små och medelstora företags förmåga att digitalisera och växa i en värld där informations-och cybersäkerhet blir allt viktigare.* Tillväxtverket, Stockholm. ISBN: 978-91-88961-68-6. Rapportnummer: 0339

[17] PwC. *Cyberhoten mot Sverige 2020*.

[18] Tillväxtverket. 2020. *Digitala affärsrisker*. Stockholm. ISBN: 978-91-88961-70-9. Rapportnummer: 0340

[19] FRA, Försvarsmakten, MSB, Polismyndigheten, PTS, Säkerhetspolisen. 2021. *Cybersäkerhet i Sverige – i skuggan av en pandemi.*

3 Metod

För att uppfylla rapportens syfte används två metoder – semi-strukturerade intervjuer och en litteraturstudie. Intervjustudien används främst för att undersöka målgruppernas behov men även för att få en uppfattning om hur målgrupperna upplever utbudet. Litteraturstudien syftar till att ge en överblick av informations- och cybersäkerhetsarbetet i företag samt det befintliga stödsystemet i form av initiativ och program för SMF. Initiativ och program som avses är tjänster, utbildning, rådgivning, coachning och diverse verktyg.

Intervjuer genomfördes med aktörer tillhörande någon av följande tre kategorier:

- Företagsfrämjare

  I kategorin *företagsfrämjare* innefattas industrikluster, science parks, inkubatorer, organisationer och företag som arbetar för att främja utveckling och tillväxt hos företag.

- Branschorganisationer

  I kategorin *branschorganisationer* innefattas branschorganisationer, vilket är en intresseförening för företag inom en viss bransch.

- Företag

  I kategorin *företag* innefattas små och medelstora företag som på olika sätt berörs av cybersäkerhet.

Intervjuerna var semistrukturerade, vilket innebär att en intervjumall med förbestämda frågor följdes, – dessa går att läsa i bilaga 2 – men som även kompletterades med icke-förutbestämda frågor i de fall då det var relevant för rapportens syfte. För att studien skulle kunna genomföras inom rimligt tidsintervall behövde ett urval göras utifrån de målgrupper som fanns. Ett antal företagsfrämjare, branschorganisationer samt företag valdes därför ut, baserat på Linköping Science Parks, Blue Science Parks och Tillväxtverkets nätverk och andra aktörer genom dessa.

Litteraturstudien baseras på rapporter som berör områdena:

- Digitalisering
- Cyberhot
- IT-säkerhet samt informations-och cybersäkerhet

Se *bilaga 1* för lista på deltagare i intervjustudien.

3.1 Metoddiskussion

Intervjustudien har en relativt stor bredd med flertalet branschorganisationer, företagsfrämjare och företag verksamma inom olika branscher. Trots att bredden är stor så är ändå urvalet – framför allt för företagen – väldigt litet sett till målpopulationen. Syftet med intervjuerna är dock inte att ge en exakt överblick av vad alla tycker och tänker utan i stället att ge ett djupare perspektiv på mer specifika problem som upplevs. Den urvalsgrupp som används i denna rapport bör vara tillräckligt stor för att uppfylla de krav som ställs på rapporten. För att få en större överblick av vad målpopulationen har för åsikter, behov och kompetens gjordes även en litteraturstudie. Litteraturen utgörs av publicerat material inom valda områden (se ovan) och bör anses vara trovärdig.

4 Behov

Att det finns ett stort behov av olika typer av cybersäkerhetslösningar kan tänkas vara en självklarhet, men det blir än mer tydligt presenterat i PwCs rapport om cybersäkerhet i Norden. I rapporten framgår det att så många som 8 av 10 svenska bolag uppger att de har varit utsatta för minst en informationssäkerhetsincident under 2020, samtidigt som var tredje bolag även uppger att de varit utsatt för fler än fem incidenter under 2020. PwC gjorde även en bedömning gällande att det, trots den redan höga andelen utsatta, även finns ett stort mörkertal i antalet utsatta för en informationssäkerhetsincident[20]. MSB menar även att den pågående pandemin har inneburit nya eller förändrade hot för företagen i och med den påskyndade digitaliseringen som pandemin har inneburit för många företag, samtidigt som de gamla hoten fortfarande finns kvar. Detta bidrar till att en framtida kris kan få allvarligare konsekvenser om företagen inte lyckas komma till rätta med både de gamla och nya sårbarheterna[19].

Att generalisera behov för företag inom området cybersäkerhet är givetvis inte enkelt då de olika företagens behov kan skilja sig markant. Exempelvis skulle man kunna tänka sig att ett företag som arbetar med stora mängder information och även arbetar digitalt i alla eller stora delar av företaget har annorlunda behov än ett företag som inte hanterar några stora mängder information och inte heller arbetar digitalt.

Kategoriuppdelningen följer tidigare nämnd uppdelning, där det i delkapitel 4.3 Övriga företag även omfattar behov som berör både tech-företag och produkt- eller tjänsteutvecklande företag samtidigt.

4.1 Tech-företag

Av de kategorier som innefattades i denna rapport så kan man tänka sig att tech-företag är den kategori med högst IT-mognad, detta gör dock inte dessa företag immuna mot cyberhot utan i stället visade många av intervjuerna – främst med företagen själva – snarare tvärt om, det vill säga att den höga digitaliseringsgraden som tech-företag ofta har kan leda till en ökad hotbild.

I intervjuerna med bland annat företagen och företagsfrämjarna så lyftes det att tech-företag ofta kunde ha ett stort säkerhetstänk med många integrerade säkerhetslösningar i deras system. Trots att man från företagens sida upplevde att systemen som användes var säkra, så fanns det en rädsla att outbildad personal skulle kunna utsättas för riktade attacker, exempelvis en phishing-attack. Detta då trots att systemen upplevs säkra, så finns risken att omedveten personal kan råka delge tillgänglighet till information eller viktiga delar av ett system. Detta är något som även stärks i rapporten *Det digitaliserade Sverige – så in i Norden säkert?* som PWC publicerat. Där nämner man att ”Den ovetande arbetaren”, det vill säga att en ovetande medarbetare omedvetet skadar bolaget, är den största oron bland svenska företag[20]. Kopplat till detta så var något som återkommande togs upp i intervjuerna just behovet av utbildningar som riktades till personal som helt saknar kompetens inom cybersäkerhet, men i många fall även inom teknik generellt.

När det kommer till tech-företagen så verkar det också finnas ett behov av kunskap på en högre nivå, eller i varje fall på en nivå som är högre än det som idag existerar. I intervjuerna med branschorganisationerna och företagsfrämjarna så framkom det att både

[20] PWC. 2020. Det digitaliserade Sverige – så in i Norden säkert?

branschorganisationer och företagsfrämjare som riktar in sig på tech-företag upplever att många teknikföretag har en IT-mognad – då även inom cybersäkerhet – som är högre än hos branschorganisationerna och företagsfrämjarna. Detta leder i sin tur till att branschorganisationerna och företagsfrämjarna upplever att de inte kan bidra med någon ny kunskap eller information till tech-företagen.

Sammanfattningsvis lyftes följande behov relaterat till tech-företagen:

- Ett behov av ett fortsatt arbete med att utveckla kompetensen hos alla medarbetare på ett företag för att minimera risken med att en ovetande arbetare omedvetet skadar företaget.
- Ett behov av kunskap på en mer avancerad nivå som är riktad till tech-företag som idag har en högre IT-mognad än de branschorganisationer och företagsfrämjare som erbjuder kurser inom cybersäkerhet.

4.2 Produkt- eller tjänsteutvecklande företag

I intervjuer med branschorganisationer och företagsfrämjare lyftes det ofta att de produkt- eller tjänsteutvecklande företagen har ett generellt behov av mer grundläggande information om cybersäkerhet. I många fall upplevs det som att dessa företag inte är medvetna om de risker som existerar vilket helt enkelt leder till att företagen inte vet vad de behöver göra för att skydda sig mot cyberhot.

Det framkom också i intervjuerna med företagen att många produkt- eller tjänsteutvecklande företag la en stor tillit till att deras leverantörer levererar digitala tjänster och mjukvara som var säkra utan att nödvändigtvis vara medvetna hur detta kan kontrolleras. Företagen har där av ett behov att kunna validera om digitala tjänster eller mjukvara som levereras är tillräckligt säker för det syfte som de är menade att användas till.

Genom samtalen med företagsfrämjare och SMF framgick även att en del efterfrågar utbildningar som sträcker sig över en längre period. Då blir det lättare att behålla kunskapen som fås under dessa och även få in rutiner för arbetet. En efterfrågan på program där en säkerhetskunnig kan under en längre period hjälpa företag att sätta sig in i ett företags olika säkerhetsaspekter specifika för företaget, och etablera rutiner kring företagsspecifika frågor framgick även.

Sammanfattningsvis lyftes följande behov relaterat till de produkt- eller tjänsteutvecklande företagen:

- Ett behov av en grundläggande förståelse kring vad cybersäkerhet är och varför det är viktigt.
- Ett behov av att kunna validera eller förstå hur säker en digital tjänst eller mjukvara är som de fått levererade av en tjänste- eller mjukvaruleverantör.
- En efterfrågan på utbildning eller program som sträcker sig över en längre tid som är företagsanpassat.

4.3 Övriga företag

I Svensk Handels rapport *Handelns utsatthet för IT-relaterad brottslighet* nämner man att bolagen inom handeln har kunskapsbrister när det kommer till grundläggande

säkerhetsfrågor och säkerhetsrutiner. Ett behov som Svensk Handel lyfter att företag inom branschen har är kontinuerlig utbildning inom hela företaget då IT-brottsligheten ständigt förändras och utvecklas. I samma rapport nämner även Svensk Handel att det finns ett behov att avstigmatisera utsattheten så att personal vågar prata och berätta om både kunskapsbrister och fall då man blivit utsatt då konsekvenserna av att inte våga ta upp det ofta är mycket värre än om utsattheten sker i tystnad. [21]

Vid en kartläggning av digital säkerhet i jordbruket genomförd våren 2021 identifierades behov att öka småföretagarnas medvetenhet kring riskerna teknik kan föra med sig, sprida information om säkerhetsåtgärder, klargöra vem som äger datasystem samlar in, samt att teknisk support är lättillgänglig efter ny teknik köpts in[22]. Det finns även ett behov att småföretagen snabbt får hjälp om en IT-incident skett. I kartläggningen framkom det vidare att småföretagens digitaliseringsarbete berodde till stor del på teknikintresset hos medarbetarna, vilket generellt sätt var större bland de yngre generationerna. En utmaning många lantbruksföretagare belyste var de stora initiala investeringar som krävs för att digitalisera verksamheten, samt att det är svårt att se nyttan säkerhetslösningar för med sig relativt kostnaden för dessa.

I Tillväxtverkets rapport *Digitala affärsrisker* nämns också att just de små tillväxtbolagen har svårt att inse vad de har att vinna på utbildning och kompetensutveckling inom cybersäkerhet[18]. Detta är även något som lyftes i flertalet intervjuer med branschorganisationerna och företagsfrämjarna, och man pekade framför allt på att man upplevde en ovilja hos de små tillväxtbolagen att lägga ner tid eller spendera pengar på de utbildningar som redan idag existerar. Ett behov som existerar för de små tillväxtbolagen är således att på ett enkelt sätt kunna ta del av information och få en förståelse kring vikten av cybersäkerhet.

Sammanfattningsvis lyftes följande behov relaterat till de övriga företagen:

- Ett behov av kontinuerlig utbildning inom hela företaget
- Ett behov av att avstigmatisera utsattheten
- Ett behov av att på ett enkelt sätt kunna ta del av information och få en förståelse kring vikten av cybersäkerhet.

[21] Svensk Handel. 2020. *Handelns utsatthet för IT-relaterad brottslighet.*

[22] Andersson, N; Lohm, E. *Säker digitalisering för lantbruket*. Agtech innovation nr 9. LiU-Tryck, Linköping 2021. ISBN 978-91-7929-029-0

5 Kartläggning av utbud

Nedan redovisas utbud av initiativ, informationsblad, utbildningar, tjänster och liknande inom informations- och cybersäkerhet som riktar sig mot SMF. En del av det utbud som redovisas riktar sig inte enbart mot SMF utan mot en större målgrupp som SMF är en del av. Utbudet är indelat i sju kategorier;

- Initiativ
- Informationsblad, rapporter och checklistor
- Tester
- Certifieringar
- Försäkringar
- Utbildningar
- Konsulttjänster

Kartläggningen av utbudet kan inte anses komplett då relevanta delar kan saknas. Om information eller erbjudanden saknas har det varit svårt att finna dessa under kartläggningen, vilket även innebär det troligtvis är svårt för företagen att hitta informationen eller erbjudandet.

5.1 Initiativ

Fyra myndigheter, i samverkan med ytterligare tre, fick i uppdrag att inrätta Sveriges nationella cybersäkerhetscenter i syfte att stärka landets ”förmåga att förebygga, upptäcka, och hantera antagonistiska cyberhot mot Sverige”[23]. Centret ska bland annat underlätta informationsutbyte mellan olika aktörer inom cybersäkerhet, tillhandahålla lägesbilder avseende hot och sårbarheter, samt ge stöd om hur verksamheter kan skydda sig mot cyberattacker. Det är även tänkt att centret ska erbjuda kompetenshöjande insatser så som övningar och utbildningar. Om och hur centret kan agera som stöd för SMF återstår att se då centret ska byggas upp under en femårsperiod för att ge effekt 2025.

För att utveckla kompetensen inom cybersäkerhet etablerar även Research Institutes of Sweden (RISE) ett centrum för cybersäkerhet[24]. Syftet är att centret, som kommer finnas i Luleå, ska agera som neutral partner för industri och offentlig sektor och stötta nätverkande, marknadsutveckling, forskning, och innovation. RISE driver även sedan slutet av 2020 en nationell nod för cybersäkerhet som ska bidra till en säker digitalisering i svenskt näringsliv[25]. SMF är en av innovationsnodens sex olika målgrupper, vars ”cybersäkerhetsbehov ska klarläggas och bemötas”. Cyber range, som också drivs av RISE, är en testbädd där företag kan testa system i en virtuell miljö för att kunna skapa säkra IT-system[26]. Testbädden tillgängliggör test- och demomiljöer för cybersäkerhet som många mindre företag ofta saknar resurser för.

Oktober är EU:s informationssäkerhetsmånad, och i Sverige genomförs ”Tänk säkert”-kampanjen som riktar sig till privatpersoner och mindre företag[27]. Enligt MSB är syftet att ”öka medvetenheten om informations-och cybersäkerhetsfrågor” samt att genom konkreta

---

[23] Centret för cybersäkerhet. U.å. *Nationellt cybersäkerhetscenter - Om centret.* https://www.cfcs.se/om-centret

[24] RISE. 2021. *RISE startar Centrum för cybersäkerhet.* https://www.ri.se/sv/press/rise-startar-centrum-for-cybersakerhet

[25] Se https://cybernode.se/

[26] Se https://www.ri.se/sv/cyberrange

[27] MSB. 2020. *Tänk säkert.* https://www.msb.se/tanksakert/

tips ”kunna vidta åtgärder för ett säkrare uppkopplat liv”. Aktiviteter som genomförts inom ramen för kampanjen är bland annat webbseminarium, säkerhetstest för företagare, filmer, föreläsningar, montrar på mässor, samt företagsevent.

CYNIC är ett initiativ mellan Luleå Tekniska universitet i Sverige och Centria i Finland som bland annat stödjer regionala SMF inom informations- och cybersäkerhet[28]. Genom att erbjuda seminarier, workshops, och evenemang är förhoppningen att höja kunskapen om digital säkerhet. Projektet utgår från två informationssäkerhetslabbar som erbjuder en dynamisk testbädd för SMF där företagen kan testa programvara och bedöma eventuella säkerhetsproblem. I labbmiljöerna kan realistiska situationer spelas upp där ”system sedan stressas och användarna lär sig vad som kan hända, hur de reagerar, och hur de kan reagera på ett bättre sätt”[29]. Liknande koncept har även genomförts på andra områden i Sverige. Linköping Science Park har genomfört en pilotutbildning inom cybersäkerhet för SMF[30]. Målet med projektet var att öka företagens medvetenhet och kunskap om cybersäkerhet, för att på lång sikt skapa bättre beredskap hos svenska innovationsbolag. Utbildningen berörde olika områden, bland annat datahantering, risker, samt hur säkerhet kan integreras i ett tidigt skede i både produkt- och affärsutveckling.

På hemsidan informationssäkerhet.se erbjuds stöd från myndigheter inom informationssäkerhet. På hemsidan finns bland annat nyheter inom området, rapporter och faktafördjupningar, vägledningar, samt metodstöd för införande av ett ledningssystem för informationssäkerhet. Målgruppen är ansvarig för informationssäkerhet i verksamheter.

Sammanställning av initiativ.

Ansvarig aktör	Initiativ	Kategori
FRA, Försvarsmakten, MSB, Säkerhetspolisen, PTS, Polismyndigheten, och FMV	Nationellt cybersäkerhetscenter	Center
	Informationssäkerhet.se	Hemsida
RISE	Centrum för cybersäkerhet	Center
	Cybernode	Nod
	Cyber range	Testbädd
MSB	Tänk säkert	Kampanj
LTU och Centria Yrkeshögskola	CYNIC	Projekt
Linköping Science Park	Pilotutbildning inom cybersäkerhet	Projekt

[28] European Commission. *CYNIC: helping SMEs develop better cyber security* https://ec.europa.eu/regional_policy/en/projects/Sweden/cynic-helping-smes-develop-better-cyber-security

[29] Alfredsson, L. 2020. *CYNIC - Företagsmodeller för digital innovation och informationssäkerhet.* LTU. https://www.ltu.se/research/subjects/information-systems/Pagaende-projekt/CYNIC-Foretagsmodeller-for-digital-innovation-och-informationssakerhet-1.180027

[30] Linköping Science Park. U.å. *Cyber Security*. https://linkopingsciencepark.se/project/cyber-security/

5.2 Informationsblad, rapporter, & checklistor

I rapporten *Informationssäkerhet för små företag* ger myndigheten för samhällsskydd och beredskap (MSB) rekommendationer för företag med upp till 10 anställda hur de kan förbättra informationssäkerheten i företaget[31]. Rapporten innehåller praktiska tips på hur information ska skyddas samt vad som ska göras ifall företaget råkat ut för vanliga cyberincidenter. Rapporten behandlar bland annat virusskydd, säkerhetsuppdateringar, molntjänster, utpressning och skydd av trådlöst nätverk. Det redovisas även steg-för-stegåtgärder av fyra bedrägerier – Id-kapning, utpressningsvirus, företagskapning samt fakturabedrägeri.

Säkerhetspolisen redovisar i sin rapport *Vägledning i säkerhetsskydd - Informationssäkerhet* rekommenderade säkerhetsåtgärder för verksamheter samt hur de kan förhålla sig till informationssäkerhet i stort[32]. Viss förkunskap kan krävas för att ta till sig innehållet i vägledningen, varpå rapporten inte är lämplig för SMF med låg kompetens inom området. Vägledning redovisas inom områden så som hantering av säkerhetskänsliga uppgifter, informationssystems arkitektur, incidenthantering samt kontroll av åtkomst och behörigheter.

Inom ramen för det nationella centret för cybersäkerhet publicerades rapporten *Cybersäkerhet i Sverige 2020 – rekommenderade säkerhetsåtgärder* där åtgärder för en säker IT-miljö presenteras[33]. Rekommendationerna är menade att utgöra ett stöd i prioriteringar i säkerhetsarbetet och inte att ersätta ett systematiskt säkerhetsarbete. Rekommendationer som ges täcker områden så som säkerhetsuppdateringar, säkerhetskopior, behörighet- och autentiseringsfunktioner, segmentering av nätverk samt förmåga att upptäcka säkerhetshändelser. Innehållet vänder sig till medarbetaren som är ansvarig för IT-miljön, och trots att målgruppen inte är SMF så kan rekommendationerna användas av organisationer utöver tänkta målgruppen (myndigheter, kommuner, och regioner). MSB & Polisen har i samverkan gett ut ett informationsblad innehållande checklistor som kan användas av företag för att förbättra säkerheten[34]. Checklistorna berör områden så som skydd mot skadlig kod samt skydd mot att obehöriga får access till värdefull information.

Stöldskyddsföreningen (SSF) erbjuder guider inom grundläggande cybersäkerhet[35]. Sex områden berörs, exempelvis hur nätverk kan skyddas, kontroll av behörigheter och informationssäkerhet vid upphandling av IT-relaterade tjänster. SSF erbjuder även guide inom förebyggande av bedrägerier, där bland sätt att undvika ransomware och bluffakturor beskrivs[36]. Under 2020 publicerades även en guide inom företagsbedrägerier med fokus på hur företag kan skydda sig mot de ökade antalen bedrägerier i samband med coronaviruset.

Många företag som erbjuder tjänster inom IT-, informations- och cybersäkerhet har guider om grundläggande steg mot en säker IT-miljö som SMF kan ta del av. Exempel är Cygate

---

[31] MSB. 2018. *Informationssäkerhet för små företag: rekommendationer för dig som driver eget företag med upp till 10 anställda*. ISBN: 978-91-7383-886-3

[32] Säkerhetspolisen. 2020. *Vägledning i säkerhetsskydd – Informationssäkerhet.*

[33] FMV, FRA, Försvarsmakten, MSB, Polismyndigheten, PTS, och Säkerhetspolisen. 2020. *Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder*.

[34] MSB och Polisen. 2020. *Tänk säkert – så skyddar du ditt företag*.

[35] Guiderna finns att hämta på https://www.ssfcybersakerhet.se/sakerhetsguide-for-it-sakerhet/

[36] Guide finns att läsa på https://www.stoldskyddsforeningen.se/foretag/sakerhetsguider/cybersakerhet/forebygg-bedragerier/

(Telia)[37], Advenica[38] och Conscia[39]. Det finns även rapporter och guider utgivna av föreningar och organisationer. Exempel på detta är Säkerhetsbranschens broschyr om cybersäkerhet och informationssäkerhet med fokus på kamera[40], Teknikföretagens guide till medvetet säkerhetsarbete i mindre teknikföretag[41], och Internetstiftelsens guide #29 om internets baksida och hur företagare kan skydda sin verksamhet[42].

[37] Se https://www.cygate.se/cybersakerhetsguide/

[38] Advenica. 2021. *8 råd till dig som ska börja arbeta med informationssäkerhet.* Doc. no.: 19356 v1.0

[39] Guider finns att hämta hem på https://conscia.com/se/whitepapers/

[40] SäkerhetsBranschen. U.å . *Cybersäkerhet – med fokus på kamera*.

[41] Teknikföretagen. 2019. *Skydda din IT-miljö – En guide till medvetet säkerhetsarbete i mindre teknikföretag*.

[42] Nyman, A. 2016. *Internetguide #29 – Skydda ditt företag mot bedragare*. Internetstiftelsen

Sammanställning av informationsblad, rapporter, och checklistor.

Utgivare	Namn	Innehåll
MSB	*Informationssäkerhet för små företag* (2018)	• Rekommendationer: ○ Skydd av enheter & företagsinformation • Steg-för-stegåtgärder: ○ Id-kapning ○ Utpressningsvirus ○ Företagskapning ○ Fakturabedrägeri
Säkerhetspolisen	*Vägledning i säkerhetsskydd - Informationssäkerhet* (2020)	• Vägledning inom informationssäkerhet: ○ E.g., hantering av säkerhetskänsliga uppgifter, utveckling av informationssystem, drift & underhåll, samt uppföljning & kontroll
FMV, FRA, Försvarsmakten, MSB, Polismyndigheten, PTS, och Säkerhetspolisen	*Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder* (2020)	• Rekommendationer inom 10 områden: ○ Säkerhetsuppdateringar ○ Behörighet-& autentiseringsfunktioner ○ Systemadministrativa behörigheter ○ Inaktivering av oanvända tjänster & protokoll ○ Säkerhetskopior ○ Utrustning i nätverk ○ Vitlistning ○ Segmentering ○ Uppgradering av hård-& mjukvara ○ Upptäckt av säkerhetshändelser
MSB och Polisen	*Tänk säkert – Så skyddar du ditt företag* (2020)	• Checklistor för: ○ Skydd mot nätfiske & skadlig kod ○ Säkra lösenord ○ Säkra kortuppgifter ○ Säkra företagets information (säkerhetskopiering, trådlösa nätverk, säkerhetsuppdatering)
SSF	*Guide till grundläggande cybersäkerhet* (u.å)	• Guider inom sex områden: ○ Datorer & mobila enheter ○ Programvaror & applikationer ○ Nätverk ○ Externa IT-tjänster ○ Behörigheter ○ Utbildning
	Förebygg bedrägerier (2019) och *Företagsbedrägerier i samband med coronaviruset* (2020)	• VD-bedrägerier • ID-kapning (mot kund & företag) • Interna bedrägerier • Ransomware • Bluffakturor

5.3 Tester

MSB och SSF har tillsammans skapat ett test som tillåter företag att få en indikation på hur bra företagets IT-säkerhet är[43]. Självtestet täcker sex områden och ger de anställda en uppfattning om cybersäkerheten i organisationen. Det finns även ett säkerhetstest framtaget för verksamt.se som går igenom digitala risker företagare behöver känna till – exempel skydd av information och hur bedrägerier kan undvikas[44].

Likt det som nämndes i kapitel 5.2 erbjuder en del konsultföretag med tjänster inom IT-informations- och cybersäkerhet självtester på sina hemsidor. Exempelvis erbjuder If ett kort test inom IT-säkerhet för företagsanställda[45]. Efter testet ges tips på vad företaget kan förbättra. Ett annat snabbtest som ger indikation på företagets cybersäkerhet erbjuds av Cygate, som efter genomfört test redovisar hur resultatet skiljer sig mot andra organisationer verksamma inom samma område[46].

Sammanställning av tester.

Utgivare	Innehåll	Omfattning
MSB och SSF	• Datorer och mobila enheter • Mjukvaror och applikationer • Nätverk • Externa IT-tjänster • Behörigheter • Utbildning i IT-och Informationssäkerhet	Berör sex områden och tar ungefär tio minuter att genomföra
Verksamt.se	• Skydd av information • Bedrägerier	Åtta frågor
If	IT-säkerhet	Tio frågor
Cygate	Cybersäkerhet	
Advenica	Utvärdering av företagets säkerhet	Sju frågor

[43] Se https://www.ssfcybersakerhet.se/testa-din-it-sakerhet/

[44] Se https://sakerhetstestet.se/

[45] If. U.å. *Testa vad du vet om IT-säkerhet.* https://www.if.se/foretag/forsakringar/ansvarsforsakring/databrottsforsakring/databrott/it-sakerhetstest

[46] Se https://www.cygate.se/tryggitmiljo/

5.4 Certifieringar och standarder

Svensk Brand- och Säkerhetscertifiering (SBSC) erbjuder en certifiering inom cybersäkerhet kallad SSF 1101 Cybersäkerhet BAS[47]. Normen för certifieringen har tagits fram av SSF i ett samarbete mellan Polisen, MSB samt branschorganisationer, och anger grundläggande krav av IT-säkerhet för SMF. Certifikatet är giltigt i tre år. SSF 1100 Certifierad Informationssäkerhetskonsult (CISK) riktar sig istället till personer med kompetens inom IT- och informationssäkerhet och vägleder företag att införa säkerhetsåtgärder enligt SSF 1101[48].

ISO 27000-serien består av olika standarder inom informations- och cybersäkerhet samt dataskydd och kan ”tillämpas inom alla organisationer oavsett bransch, storlek och verksamhet”[49]. Serien stödjer bland annat införande av säkerhetsåtgärder för att skydda information. Företag kan certifiera sig mot ISO/IEC 27001.

Common Criteria for Information Technology Security Evaluation (CC) är en standard för utvärdering av säkerheten hos IT-produkter[50], och kan användas för att opartiskt beskriva och utvärdera IT-säkerheten på ett kontrollerbart och tydligt sätt.

Sammanställning av certifieringar och standarder.

Utgivare	Namn
SBSC	SSF 1101 Cybersäkerhet BAS
	SSF1100 Certifierad Informationssäkerhetskonsult
ISO	SS-ISO/IEC 27000
	Common Criteria (CC) - ISO/IEC 15408

[47] SBSC. U.å. *SSF 1101 Cybersäkerhet BAS*. https://www.sbsc.se/certifikat/ssf-1101-cybersakerhet-bas/

[48] SBSC. U.å. Certifierad Informationssäkerhetskonsult. https://www.sbsc.se/certifikat/certifierad-informationssakerhetskonsult-cisk/

[49] SIS. U.å. *Detta är ISO 27000*. https://www.sis.se/iso27000/dettariso27000/

[50] MSB. 2019. *Common Criteria*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/standardisering-inom-informationssakerhet/common-criteria/

5.5 Försäkringar

Det finns ett antal försäkringar från olika försäkringsgivare som är gjorda för att stödja företagare vid cyberbrott. I försäkringarna ingår det i de flesta fallen bland annat utredning av intrånget och stöd för att komma i gång igen, ersättning för förlorad inkomst när verksamheten står still och stöd vid betalning av skadestånd. Flera av dessa försäkringar ingår i företagsförsäkringen som erbjuds av försäkringsgivarna. Liknande tjänster kan ingå i en vanlig företagsförsäkring även om försäkringsgivaren inte har en uttalad Cyberförsäkring.

Sammanställning av försäkringar.

Företag	Försäkring
Länsförsäkringar	Dataskyddsförsäkring
If	Databrottsförsäkring
Trygg Hansa	Cyberförsäkring
Aon	Cyberförsäkring
AIG	CyberEdge Cyberförsäkring
Moderna	Cyberförsäkring

5.6 Utbildningar

Nedan listas ett urval av de tillgängliga utbildningarna som finns inom ämnet. Enbart en är uttalat riktad mot SMF och därför behöver företagen själva veta vilka utbildningar som är relevanta för dem från det befintliga utbudet.

Vidare erbjuds utbildningar inom ämnet av fler företag som exempelvis Secure state cyber och Nimblr men mer information om utbildningarnas innehåll och omfång ges på begäran. Mer specifika utbildningar ges av företagen som listas nedan med och detta är inte deras fullständiga utbildningsutbud.

Universitet och högskolor erbjuder också kurser inom informations- och cybersäkerhet. Dessa söks som privatperson och kan ställa olika förkunskapskrav samt att individen som söker möter antagningskraven.

Sammanställning av utbildningar.

Utgivare	Namn	Pris (SEK)	Omfång	Målgrupp
SSF	Cybersäkerhet – Bas Utbildning	9 500	1 dag	SMF
	Säkerhet bas – Utbildning	16 300	2 dagar	Chefer/anställda som jobbar med säkerhetsfrågor
MSB	Kurs i strategisk och systematisk informationssäkerhet	5 200	3/6 dagar	Chefer/CISO
	Grundkurs i säkerhet i industriella informations- och styrsystem	Gratis	2 dagar	Utvecklingsingenjörer/operatörer inom information och styrsystem
	Informationssäkerhet - Operativ informationssäkerhets-kurs	Gratis	2-3 minuter i veckan i 14 veckor	Personal som arbetar med säkerhetsfrågor
	Informationssäkerhet - Taktisk informationssäkerhets-kurs	Gratis	5 minuter i veckan i 13 veckor	CISO
	Digital informationssäkerhets-utbildning för alla (Disa)	Gratis	Materialet finns tillgängligt online och gås igenom som önskas	Alla
Secify	Informationssäkerhet – motståndskraft genom medvetenhet	Pris vid förfrågan	2 timmar	Alla

	Informationssäkerhet – motståndskraft med praktiska verktyg	Pris vid förfrågan	4 timmar	Alla
	IT-säkerhet – teknisk säkerhet	Pris vid förfrågan	4 timmar	Alla
	IT-säkerhet – teknisk säkerhet på djupet	Pris vid förfrågan	4 timmar	IT-avdelningen
SIS	Grunderna i informationssäkerhet - steg 1 enligt ISO 27000	22 900	3 dagar	Ansvariga för informationssäkerhetsfrågor

5.7 Konsulttjänster

Det finns många konsultföretag som erbjuder tjänster inom IT-, informations- och cybersäkerhet, men alla dessa är inte relevanta för SMF. För att se vilka som erbjuder konsulttjänster till SMF se sammanställningen av företag och ett urval av deras tjänster nedan.

Sammanställning av konsulttjänster.

Företag	Tjänster
2secure	Penetrationstester, riskhantering, kodgranskning och molnsäkerhet.
4C strategies	Sårbarhetsbedömning, riskövervakning, bedömning av cybersäkerhetsmjukvara och kompetensutveckling.
Basalt	Riskbedömning och granskning av nuvarande IT-system.
Combitech	Säkerhetstestning, systemövervakning, säkerhetsgranskning.
Cybercom	Penetrationstester, molnsäkerhet och sårbarhetsskanning.
IT-Total	Bedömning och testande av nuvarande IT-system, rådgivning och experthjälp vid misstanke av intrång och cyberattack.
Knowit	Helhetsleverantör inom cybersäkerhet och relaterad juridik.
Outpost24	Applikations och DevOps säkerhetstestande, nätverkssäkerhet och molnsäkerhet.
Rote Consulting AB	Säker och effektiv informationshantering.
Secify	Risk- och sårbarhetsanalys, riskcheck penetrationstester.
Truesec	Kodgranskning, penetrationstester och utvärderingar av phishing-risk.
Yes it networking solution	IT-säkerhetstjänster, Coachning, GDPR.
Weop	Informationssäkerhetsanalyser och utbildning inom informationssäkerhet.
West code solutions	Rådgivning.

5.8 Internationell utblick

Utöver det utbud som hittills presenterats i kapitel 5 så kan svenska SMF även finna stöd från organisationer i andra länder eller från internationella aktörer. Exempelvis har Center for Internet Security (CIS) tagit fram en rapport med praktiska råd på hur man kan säkra sitt företag[51]. Rapporten är uppdelad i tre delar; grundläggande, fundamental och organisatorisk. Råden är djupgående även i den grundläggande delen och inte lika konkreta som de råd som ges i MSB:s rapport *Informationssäkerhet för små företag*. Ett annat exempel på stöd SMF kan finna internationellt är en checklista utgiven av Financial Industry Regulatory Authority (FINRA) för att hjälpa små företag att bli säkrare[52]. Checklistan är baserad på FINRA:s rapport om arbete inom cybersäkerhet och National Institute of Standards and Technologys (NIST) ramverk för cybersäkerhet. Det EU-finansierade initiativet Digital SkillUp erbjuder också stöd till SMF i form av bland annat online-utbildningar (där cybersäkerhet är en av de tre fokusområdena) och har som syfte att hjälpa SMF lära sig mer om ny teknik och underlätta digital transformation[53].

Genom kontakt med Blue Science Parks nätverk har det framgått att flera av Sveriges grannländer har precis som Sverige branschföreningar som samlar cybersäkerhetsindustrin, däribland InfoBalt i Litauen och FISC i Finland. Även TeleTrust i Tyskland och CenSec i Danmark har liknande roller, men har en bredare roll utöver ren cybersäkerhet. I Litauen äger deras Försvarsdepartement, Litauen Ministry of Defence, frågan som helhet, och har information, guider och utbildningar. Uppfattningen är att MoD erbjuder fler aktiviteter och därmed når ut bra till SMF. Det är enskilda privata bolag som tillhandahåller tjänster. I Norge finns NorSIS, som är en del av regeringens satsning på informationssäkerhet i landet, och tillhandahåller aktiviteter inom området åt privat och offentlig sektor. Det finns även en satsning för att få ungdomar och lärare mer intresserade av cybersäkerhet genom projektet Cybersmart, som verkar för en bättre digital säkerhetskultur.

Genom kontakt med nätverket IASP, international Association of Science Parks and Areas of Innovation, framgick att exempelvis en Science Park i Spanien får förfrågningar om support från SMF angående cybersäkerhet, så som policys, hur man gör back up, hanterar lösenord på ett säkert sätt och hur internet och mail kan användas säkert. Science Parken erbjuder rådgivning inom området. Även om detta exempel förstås inte kan representera en större mängd, fås en inblick i att andra aktörer känner av ett behov kring stödsystem inom cybersäkerhet för SMF.

I Nederländerna finns ett ”Digital Trust Center”, framtaget av ”the Ministry of Economic Affairs and Climate Policy” och ”the Ministry of Justice and Security”, som har två huvudsyften. Det första är att erbjuda företag oberoende information om digitala sårbarheter och konkreta förslag på vilka åtgärder företagen ska ta för att minska den digitala sårbarheten samt att agera som en digital plattform som uppfyller detta syfte. Det andra är att främja cybersäkerhetsallianser mellan företag. Digital Trust Center har flera erbjudanden till både små och stora företag och ett av erbjudandena är tillgång till deras digitala plattform med aktuell och trovärdig information. Denna information består bland

---

[51] CIS. 2018. *CIS Controls*. https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF

[52] Guide finns att ladda hem på https://www.finra.org/compliance-tools/cybersecurity-checklist

[53] Bieliauskaite, J. 2021. *Digital SkillUp launches free innovative online courses on emerging technologies for SMEs and individuals.* https://www.digitalsme.eu/digital-skillup-launches-free-innovative-online-courses-on-emerging-technologies-for-smes-and-individuals/ För guide inom cybersäkerhet se https://courses.reaktor.education/en/courses/cybersecurity/overview/

annat av grundläggande riktlinjer som ska finnas till stöd i företagens arbete med cybersäkerhet, uppdaterad information kring aktuella hotbilder och hur man bör agera om man drabbas samt steg för steg guider för hur företag ska agera för att upptäcka om de blivit angripna. Digital Trust Center erbjuder även bidragssystem till företag som söker andra företag att samarbeta med kring cybersäkerhetfrågor.

5.9 Summering av utbud

Kartläggningen synliggör att stöd till SMF inom informations- och cybersäkerhet finns. Det erbjuds både kunskapshöjande och rådgivande stöd i form av bland annat guider, tester, försäkringar, utbildningar och konsulttjänster. Däremot kan en utmaning för SMF vara att spendera tid och resurser på området. Vid mer passiva hjälpmedel, så som digitala guider och tester, krävs även ett engagemang från SMF sida att söka upp och hitta dessa. En del av utbudet som presenterats i kartläggningen riktar sig mot en större målgrupp, exempelvis organisationer i stort, och även om SMF tillhör den kategorin så är utbudet inte specifikt anpassat för SMF. Frågan kvarstår om utbudet för SMF är tillräckligt i sig men att problematiken är att det inte når ut till småföretagen, eller om problematiken ligger i att utbudet måste utökas eller erbjudas i andra format.

6 Diskussion

Ett behov som lyftes relaterat till tech-företagen var att det krävs ett fortsatt arbete med kompetensutveckling av alla medarbetare på ett företag för att undvika problematik med att mindre säkerhetsutbildad personal på ett företag blir svaga länkar och mål för phishing-attacker. I kapitel 5.6 framkommer det att utbildningar inom detta ämne existerar. Frågan blir då varför behovet kvarstår. Detta behöver undersökas vidare för att se om det beror på att utbudet är för begränsat, inte är tillräckligt anpassat mot SMF eller om det bedöms vara för dyrt.

Ett behov som egentligen var generellt för flera av de små tillväxtbolagen - till viss del exkluderat tech-företagen - var en förståelse kring varför cybersäkerhet var nödvändigt över huvud taget. I intervjuerna och i litteraturen så kunde man ana att branschorganisationer, företagsfrämjare och företag hade olika syn på tillgängligheten av utbildningsmaterial och information för att öka just medvetenheten kring cybersäkerhet. I flera av intervjuerna med både företagsfrämjare och branschorganisationer så nämndes det också att det antingen redan fanns ett utbud, eller att det inte fanns ett utbud på grund av bristande intresse från små tillväxtbolag alternativt bristande kunskap hos företagsfrämjaren. Samtidigt framkom det i intervjuer med företagen att intresset att öka medvetenheten och kunskapen fanns men att utbudet antingen inte existerade, eller att kostnaderna var för höga. Hur eller varför detta glapp har uppstått är svårt att veta utan fortsatta studier inom just detta område men i kapitel 5.6 framkommer det att åtminstone en utbildning riktad till SMF existerar.

När behoven summerades för produkt- eller tjänsteutvecklande företag i kapitel 4 så nämndes att dessa företag hade ett behov av att kunna validera eller förstå hur säker en digital tjänst eller mjukvara är som de fått levererade av en leverantör. Just denna svårighet vid förhandlingar med leverantörer var något som lyftes i en intervju. Man upplever att man kan bli ”bortgjord” av säljare och har svårt att validera huruvida något är så säkert som de säger eller om det enbart är ett säljknep.

Vad som framkom i intervjuer med leverantörer av säkerhetstjänster är att man som beställare av en IT-tjänst inte kan förvänta sig att säkerheten kommer med, om man inte kravställt denna. Ur intervjuer med SMF, de som beställer IT-tjänster, framkom att flera av dem förlitar sig på att tjänsterna de köper är säkra. Huruvida tjänsten eller produkten är säker är inte heller något de kan kontrollera då kompetensen ofta saknas. Genom att inte ställa säkerhetskrav på en köpt tjänst eller produkt kan det bli svårt att som beställare skjuta över ansvaret på leverantören. Detta skulle kunna göra att säkerhetsfrågan i dessa fall hamnar mellan stolarna vilket kan resultera i en brist på säkerhet.

7 Slutsatser

Som tidigare diskuterat är Sverige ett av EU:s mest digitaliserade länder, och strävar efter att använda digitaliseringens möjligheter, något som även kommer med risker. Runtom i Sverige pågår insatser för att öka digitaliseringen, men säkerhetsfrågan är sällan högt prioriterad. Arbetet med just informations- och cybersäkerhet för SMF kan därför bli en stor utmaning.

7.1 Komplex fråga

Frågan kring Cybersäkerhet är stor och komplex. Hotbilden skiljer sig åt med allt från samordnade och systematiska attacker från stater till ett sätt för kriminella att tillskansa sig medel. Även konsekvenserna av en bristande förmåga är komplex. Det kan vara riktade attacker mot olika verksamheter som mer eller mindre kan betraktas som terrordåd som försvagar samhällsfunktioner som el- eller matförsörjning, fungerande kommunikationer eller betalsystem. Det kan även vara mer osynkroniserade störningar som virus eller bedrägerier som driver kostnader för bolagen. En annan komplexitet är att frågan är organisatoriskt allomfattande där alla individers beteende och agerande potentiellt utgör den svagaste länken. Ytterligare en komplexitet är att det finns en existerande industri av bolag som idag erbjuder marknaden produkter och tjänster inom området informations- och cybersäkerhet. Vilket uppdrag har då den offentliga sektor och vad ska marknaden hantera själv?

Ur ett nationellt perspektiv jobbar verksamheter som SÄPO och MUST för att informera och utbilda i frågan ur ett samhälles säkerhetsperspektiv. Detsamma gäller för MSB. Ur ett näringslivsperspektiv jobbar Tillväxtverket med fler, för att främja digitalisering med fokus på tillväxt och innovation. Med ett ökat antal intrång och hackerattacker både i Sverige och globalt, liksom ett eskalerande mediagenomslag för dessa händelser, riskerar vi hamna i ett ogynnsamt moment 22, där företag och verksamheter avstår digitalisering på grund av alla potentiella hot och risker som ökad uppkoppling medför. Detta kommer i sin tur att bidra till minskad tillväxt och minskad innovation – vilket i ett långsiktigt perspektiv hämmar landets tillväxt. Det vi i stället behöver är att lyfta frågan proaktivt och säkerställa att säkerhet integreras i all digital utveckling från start. Så hur fås en bättre balans? Slutsatserna i denna rapport kommer primärt fokusera på hur vi kan öka förmågan hos de aktörer som dagligdags möter SMF för att stötta dem att bli mer konkurrenskraftiga.

7.2 Kompetens finns – men har svårt att nå ut

Det finns mycket kunskap om cybersäkerhet i Sverige. Frågans aktualisering har nått politiken och fler nya satsningar har sjösatts under senare år. Bland annat Cyber range i Kista, Cyber center i Luleå, samverkan mellan fem myndigheter med mera. Dessa insatser påvisar att kunskapen finns, och behöver naturligtvis förädlas och vidareutvecklas. En utmaning är idag att den kunskap som finns idag finns i öar, och att gränssnitten inte finansieras. Detta gör att kunskapen har svårt att överföras mellan relevanta företag och organisationer, och heller inte tillgängliggörs och paketeras för att passa SMF:s behov.

Investeringar görs som beskrivits i flera parallella nationella initiativ, men de står i dag för långt ifrån målgruppen SMF. Det är dessutom många frågor som konkurrerar om vikten på ett SMF:s strategiska agenda, där hållbarhet, kompetensförsörjning, internationalisering och jämställdhet är några av dem. Säkerhet har svårt att ta sig in på styrelse- och ledningsnivå i de små bolagen, som förväntas fokusera på många frågor vid sidan av kärnverksamheten och har svårt att få såväl ekonomiska som personella resurser att räcka till.

Det kan finnas problem med att paketera ett budskap inom informations- och cybersäkerhet riktat till en bred målgrupp. Förutsättningarna är olika mellan branscher, men de är även olika mellan olika företag. Organisation, tillväxtfas och kultur påverkar hur företag tar till sig och jobbar med säkerhetsfrågan. Myndigheter, forskningsinstitut eller branschorganisationer kan få svårt att tillgodose behovet själva. Det finns också en övertro på checklistor som ska lösa informationsbehovet för en så viktig fråga. Det behöver riktas finansiering till aktörerna som jobbar i gränssnitten, som kontinuerligt möter företagen och ser deras behov, och som har ett brett kontaktnät med akademi och samhälle – och vet var rätt kunskap för rätt tillfälle finns att hämta. Dessa gränssnittsaktörer har en viktig roll att spela.

7.3 Nationell samordning och regional närvaro

På det nationella planet behövs det en samordningsfunktion som har koll på vilken kompetens som finns hos olika nationella myndigheter, vid lärosäten och forskningsinstitut samt vilka de främsta privata aktörerna på området är. Det behövs överhörning, och en lärande process mellan dessa aktörer som främjar en utveckling som sker komplementärt och framtidsfokuserat, och där såväl samhällsskydd som näringslivets tillväxt tas i beaktande.

På det regionala planet behöver vi organisera oss för en effektiv spridning av kunskap och tjänster som främjar en ökad digitalisering där säkerhetsaspekterna tas i beaktande från initiala skeden och blir en naturlig del i affärs- och verksamhetsutvecklingen. En regional organisation bör byggas horisontellt och gå på tvären, ta i beaktande hur den regionala näringslivsstrukturen ser ut, vilka de största hoten och riskerna är – såväl lokalt, regionalt som nationellt – för att säkerställa ett bra proaktivt säkerhetsarbete i det regionala näringslivet. Företagsfrämjare behöver utbildas för att bära med sig perspektivet i all rådgivning och stödjande arbete som riktas till SMF. Kontakter med regionala branschorganisationer bör etableras för gott samarbete i frågan.

7.4 Var ska satsningen ske?

I denna rapport är företagen uppdelade efter hur deras erbjudande ser ut. Några viktiga slutsatser är att det ligger ett stort ansvar på tjänsteleverantörer av olika IT-lösningar. Alla bolag pekar på sina leverantörer snett uppåt. Det lilla bolaget utgår ifrån att sin leverantör levererar säkert, där denna leverantör i sin tur utgår ifrån att sin leverantör är säker, och så vidare. Många leverantörer tycker även att det behövs bättre beställarkompetens. Många IT-produkter och tjänster är väldigt enkla att köpa och installera, när allt fungerar bra. Detta har betytt att beställarkompetens inte har varit nödvändig att ha inom IT-området. Företag ser därför inte egen IT-kompetens som en nödvändighet. Ekonomichefen vet vilka funktioner som krävs av ett ekonomisystem, men inte vilka krav de ska ställa på BackUp, Redundans etcetera. En slutsats är därför att insatser bör fokuseras på leverantörer av IT-lösningar. Blir de bättre på att hantera frågan för sina kunder så kommer även risken för kunderna minskas. Detta bör även driva tillväxten hos dessa företag. Kan ett företag berätta för sina kunder hur man bidrar till en robust och säker miljö så kommer det garanterat stärka värdeerbjudandet. Insatser bör även riktas till ledning och styrelser i traditionella SMF. Företagen måste bli stöttade i att förstår hur man digitaliserar säkert och vilka kostnader och utvecklingsinsatser det kräver för bolag som helhet.

8 Förslag på framtida insatser

Förslag på framtida insatser baseras på studiens kartläggning av målgruppens behov och det utbud som finns idag. Stödet till SMF bör finnas på olika nivåer och möta gruppens behov både kortsiktigt och på längre sikt. För att uppnå detta måste initiativ finnas på olika nivåer, dels nationellt och regionalt, dels hos industrierna. Initialt måste en del av stödsystemets aktörer lära sig arbeta med småföretagen ifall de tidigare inte gjort detta, samt vara medvetna om att inkörningstiden för företagen kan vara lång då området är nytt för många. För att säkerställa att stödsystemet fyller sin funktion även i framtiden är det viktigt att insatserna kontinuerligt ses över och anpassas utifrån SMF:s behov och de digitala hoten.

8.1 Nationellt ansvar och regional spridning

För att nå ut till så många företag som möjligt, och med så bred spridning som möjligt, krävs att insatser sker både på nationell nivå och även ha en spridning regionalt och inom branscher.

8.1.1 En nationellt ansvarig

För att företagen enkelt ska hitta information kring digital säkerhet kan en aktör utses som nationellt ansvarig för informationsspridning inom informations- och cybersäkerhet riktat mot SMF. Processen för att ta fram någon aktör som tar ett större ansvar är något som i dagsläget pågår.

Ett lyckat exempel på hur en nationellt ansvarig kan finnas som stöd för företag är Nederländernas Digital Trust Center, som presenterades i 5.8.

8.1.2 Regional och branschinriktad spridning

På längre sikt skulle center på regional nivå med samlad kompetens inom informations- och cybersäkerhet kunna etableras för att få en regional spridning. Dessa säkerhetscenter kan genom löpande utbildningsinsatser och information rikta sig till företagsfrämjare i ett kunskapshöjande syfte. Genom att utbilda företagsfrämjare når kunskapen ut till en större massa. Eftersom digitalt material ofta är passivt är ett förslag att det även erbjuds material i flera format, däribland rådgivning. Ett första steg är att undersöka vilka existerande strukturer som är mest lämpliga att ge uppdraget, hur finansieringen av dessa ska gå till och ett exakt innehåll för dessa centra.

För att uppnå maximal spridning och stöd skulle det även kunna, beroende på bransch, spridas genom industrivertikaler. Det är en vanlig väg för dataintrång att gå via underleverantörer till större bolag. De större bolagen skulle därmed dra nytta av att säkerställa säkerheten genom hela sin leverantörskedja. Detta skulle kunna göras med en it-säkerhetstjänst för alla sina underleverantörer dit dessa företag kan ringa för att få hjälp vid misstanke om dataintrång, och även tillgång till olika material för att underlätta sitt säkerhetsarbete. Denna åtgärd är förstås inte applicerbar i alla branscher, då de fungerar olika, och inte heller täckande alla bolag, men skulle kunna vara ett effektivt sätt att nå ut till bolag och utnyttja kompetensen som finns.

En utgångspunkt när man bygger upp regionala kontaktpunkter bör vara att man förstärker och nyttjar existerande strukturer. Den som tar ett regionalt ansvar för att arbeta med frågan bör vara en neutral part med kompetens inom teknik och breda nätverk inom bolag såväl som i stödsystemet, företag och akademi. Exempel på existerande nationella strukturer som skulle kunna nyttjas är organisationen SISP, Swedish Inkubators & Science Parks som har 70 medlemmar, 6000 företag i sitt nätverk som representerar 95 000

anställda. Ett mer begränsat nätverk är Sweden ICT som består av de sex största Science Parkerna i Sverige, från Luleå i norr till Lund i söder.

Det finns några intressanta exempel på hur man kan jobba för att utveckla regionala kontaktpunkter med utgångspunkt från existerande strukturer.

8.1.2.1 Exempel på liknande strukturer

Energimyndigheten genomförde under 2021 en upphandling avseende ”Insatser för kommersialisering av energiinnovationer”. Upphandlingen riktades till innovationsmiljöer som fick möjlighet att i olika aktörskonstellationer genomföra insatser som genom samarbete och kraftsamling främjar samt påskyndar kommersialiseringen av energiinnovationer. Varje aktörskonstellation utvärderades dels på genomförbarheten, dels på innehållet. I många fall har konstellationerna använt denna upphandling för att vidareutveckla och mer aktivt integrera frågan om energiomställning i existerande erbjudande. En motsvarande upphandling skulle kunna göras avseende insatser inom Cybersäkerhet. Fördelen med denna struktur är att den är lättarbetad och att den stärker och vidareutvecklar existerande initiativ. Den är även administrativt enkel då den är 100 % finansierad och inte kräver medfinansiering. Nackdelen kan vara att det utvecklas många väldigt lokala initiativ med låg drivkraft att konsolideras.

Ett annat exempel är AI Sweden som finansieras av Vinnova. Målsättningen med AI Sweden är att accelerera tillämpningen av AI hos bolag. I denna modell har man tydligare valt att etablera en centralstyrd organisation med målsättning att skapa nationella samverkansstrukturer och erbjudanden. Det finns en central organisation, och sedan ett antal regionala noder, vars uppdrag är att AI Swedens erbjudande ska nå ut till företag. Dessa noder har sitt säte hos Science Parks, Universitet och kluster. Noderna ansvarar för att rekrytera kunniga partners till AI Sweden, medan den centrala organisationen ansvarar för budget och erbjudandet. Denna modell är betydligt mer komplex än Energimyndighetens och kräver fler parters inblandning för att säkerställa medfinansiering. AI Swedens modell att skapa tydligt paketerade erbjudanden har även visat sig utmanande då näringslivsstrukturen och behoven skiljer sig åt i de olika regionerna. Fördelarna är att man genom tydligt paketerade erbjudanden har access till hela nätverket.

En slutsats är att om man vill nå ut med insatser snabbt som ska integreras i existerande strukturer bör man titta närmre på den modell energimyndigheten arbetar med, vill man skapa ett paketerat nationellt program så är AI Sweden den modell man kan inspireras av.

8.2 Kunskapshöjande insatser

Behoven som finns har tydligt varit även utbildning och mer kunskap, inom flera typer av företag och branscher. För att framgångsrikt införa kompetenshöjande insatser krävs att det finns en struktur som framgångsrikt kan nå ut med erbjudanden. Denna fråga är därför starkt sammankopplad med frågan om Regionala kontaktpunkter. Att ta fram utbildningar som finns tillgängliga hos olika aktörer exempelvis på nätet är möjligen inte det mest framgångsrika. Aktualitet, relevans och incitament, skulle i stället kunna anses väldigt viktiga när det gäller kompetenshöjande insatser inom informations- och cybersäkerhet. Området inom Cybersäkerhet utvecklas i en rasande takt, där det är svårt att förutsäga morgondagens hot, som även skiljer sig mellan branscher. Utbildningar inom Cybersäkerhet måste med andra ord vara väldigt dynamiska och ske i nära samverkan med industrin för att vara aktuella. Relevansen handlar om att det måste vara relevant för den målgrupp som insatsen riktar sig till. Det handlar såväl om förkunskaper inom området som att utbildningen måste anpassas till den målgruppens egen kontext. Det bör även finnas med

incitamentsmodeller som ger målgruppen fördelar, eller undviker nackdelar, om de tar del av en kompetensutvecklingsinsats.

8.2.1 Breddutbildningar

Det finns sannolikt en marknad för att ta fram kompetenshöjande insatser som kan rikta sig till många, till exempel utbildningsinsatser till styrelser, ledningsgrupper eller utvecklingsteam. En modell värd att prova är att genom upphandlingar låta marknaden ta fram ett antal breddutbildningar. Ett problem är att det inte efterfrågas utbildningar från de flesta aktörer, vilket är varför det kan vara bra att jobba med en modell likt den som användes när man tog fram Covidvaccin. Där det offentliga tar risk genom att bekosta framtagandet av utbildning men att marknaden själv sedan får möjlighet att sälja den.

8.2.2 Integrerade utbildningsinsatser

Ett framgångsrikt sätt för främjarsystemet att utbildas samtidigt som man erbjuder sina kunder utbildning är att jobba med pilotinsatser. Genom att jobba med integrerat lärande ökar kompetensen hos bolag samtidigt som företagsfrämjarna utvecklas.

Ett liknande exempel på det är projektet Swedish Scaleups, som finansierats av Tillväxtverket. Parallellt med att erbjuda insatser till snabbväxande bolag har 10 företagsfrämjare utvecklat erbjudanden. Detta har skett inom områden som hållbarhet, kompetensförsörjning och kapitalanskaffning.

8.2.3 Incitamentsmodeller

Det finns många utbildningar idag som inte når ut. I undersökningen som gjorts för rapporten framkommer att många bolag ser en kostnad för att genomföra kompetenshöjande insatser. Det kan vara rimligt att arbeta med olika incitamentsmodeller. Man skulle likt utbildningen Elements of AI kunna ge högskolepoäng till deltagarna, det skulle sannolikt öka incitamenten hos individer för att stärka sina Cv:n. En annan modell är att man får ökad tillgång till stöd efter genomförd utbildning. Det samma skulle kunna gälla bolag eller främjare som genomfört utbildningsinsatser. Ytterligare en modell som skulle kunna fungera är att bolag får söka ersättning för förlorad arbetstid efter genomförd utbildning. För varje anställd som genomfört en utbildning skulle bolaget få ersättning.

8.2.4 Riktade utbildningar

En slutsats som gjorts genom de genomförda intervjuerna är att generella utbildningsinsatser inom informations- och cybersäkerhet inte tillför något värde utan man efterfrågar djupare kunskap och mer riktade insatser anpassade till företaget och branschen. Det kan därför vara bra att utbildningsinsatser tas fram för att möta en specifik kontext. Exempel på insatser som genomförts för specifika målgrupper är framtagande av en utbildning av Säker digitalisering inom lantbrukssektorn. Ett annat exempel är att Linköpings Science Park har genomfört en pilotutbildning inom Cybersäkerhet riktat till 20 mindre Techföretag. Resultatet av den utbildningen är ett ramverk som skulle kunna användas och anpassas även av andra målgrupper.

8.3 Help-desk funktion

Ett samlat ställe för information dit man kan vända sig med diverse frågor rörande informations- och cybersäkerhet skulle underlätta för företag som inte har egen IT-kompetens, eller saknar säkerhetsleverantör. Detta ställe skulle då kunna erbjuda en tjänst där man kan kontakta dem, likt 112, vid händelse av en cyberattack.

Om ett SMF råkat ut för en IT-incident underlättas situationen även om det finns tillgängliga guider med förslag på åtgärder. Guiderna kan vara anpassade efter incident. Leverantörer skulle kunna erbjuda guider, eventuellt som en egen produkt eller tjänst, med vad som ska göras om systemet ligger nere.

År 2018 försökte Linköping Science Park, i samtal med Combitech, lyfta frågan med inspiration från satsningen på Digital Trust Center i Nederländerna. Tanken var att bygga en helpdeskfunktion som kan drivas av ett callcenterbolag, som sedan bemannas med studenter från relevanta utbildningar vid olika universitet. På detta sätt fås färsk kompetens, och studenterna får inblick i företagens behov och frågeställningar, säkerhetsfrågans relevans och grundläggande kunskap om beredskap. Genom att samverka med ett IT-säkerhetsföretag kan denna aktör utbilda studenter, och kan även ta uppdrag av svårare karaktär där expertkunskap behövs. Även om det möjligen var för tidigt för frågan då, är idén god och ett bra komplement till den tidigare presenterade idén om regional spridning. Denna 112-funktion skulle med fördel skapas som en nationell resurs.

I dagsläget finns guider för vad som ska göras om man blir utsatt hos MSB, men dessa guider ligger i ett större informationsblad och är svårt att hitta. En idé vore att göra ett enskilt dokument med bara vad som SMF kan göra om de blir utsatta för en attack, med de olika attacker som kan ske och som är lättillgänglig. Likt diskuterat kring Svensk Handels hemsida tidigare skulle dessa guider även kunna vara branschspecifika, och finnas tillgängliga hos respektive branschorganisation.

8.4 Övrigt

I kapitel 4 kan man läsa att ett av behoven som företagen hade var att avstigmatisera utsattheten för att förhindra att anställda inte vågar berätta om de blivit utsatta för en cyberattack vilket i många fall kan förvärra situationen då den inte blir hanterad i tid. 2020 genomförde MSB kampanjen tänk säkert med syfte att öka medvetenheten om informations- och cybersäkerhetsfrågor, något som är en viktig del i att avstigmatisera utsattheten för cyberhot[54]. Ett förslag på en insats är att det skapas både fler och utökade initiativ för att öka just medvetenheten kring informations- och cybersäkerheten och för att anställda ska våga berätta om de blivit utsatta eller råkat göra ett misstag.

Genom en ökad medvetenhet förväntas attraktiviteten för ämnet också öka, vilket är viktigt för att frågan ska prioriteras hos företagen. Vidare så gör en ökad medvetenhet om vilka certifieringar som finns inom området det lättare för SMF att se vilka leverantörer som är säkra och vilka krav som kan ställas. I dagsläget efterfrågas certifieringar, vilka även finns, men det verkar som att medvetenheten kring dessa saknas.

I rapporten *Informationssäkerhet - Små och medelstora företags förmåga att digitalisera och växa i en värld där informations- och cybersäkerhet blir allt viktigare* utgiven av Tillväxtverket 2020 ger författaren många bra förslag på kompetenshöjande insatser. Några av de förslag som nämns och som även denna kartläggning anser bör studeras vidare på är konkreta ”roadmaps” med vägledning, anpassning av ramverk så som NIST och CIS så de kan användas av SMF, samt konsultcheckar för strategiskt informationssäkerhetsarbete.

[54] Se https://www.msb.se/tanksakert/

Bilaga 1. Lista på intervjudeltagare

Företag/Organisation	Intervjuperson	Tjänst/Uppdrag	Kategori
Almi Företagspartner Nord	Torbjörn Edvall	Affärsrådgivare	Företagsfrämjare
Almi	Åsa Ekman	Projektledare och affärsrådgivare	Företagsfrämjare
Anonym	Anonym	Klusterledare	Företagsfrämjare
Anonym	Anonym	Affärscoach	Företagsfrämjare
Anonym	Anonym	Utvecklingschef	Företag
Fergas Group	Magnus Pettersson	Grupp CFO	Företag
Företagarna	Pontus Lindström	Jobbar med brott och säkerhetsfrågor	Branschorganisation
High Five	Anna Petersson	Innovationschef	Företagsfrämjare
Techtank	Ingela Håkansson	Klusterledare	Företagsfrämjare
Lagafors	Magnus Elmblad	VD	Företag
LEAD	Catharina Sandberg	VD	Företagsfrämjare
Outpost24	Louise Burman	Nordenchef	Företag
Region Halland	Erik-Wilhelm Behm	Strateg	Företagsfrämjare
Stöldskyddsföreningen	Thomas Brühl	VD	Företagsfrämjare
Swedsoft	Gabriel Modeus	Generalsekreterare	Branschorganisation
Teknikföretagen	Patrik Sandgren	Näringspolitisk expert	Branschorganisation
Truesec	Mikael Lagström	Konsultchef	Företag
Östsvenska Handelskammaren	Johan Callenfors	Medlemsrelationer och affärsutveckling	Företagsfrämjare

Bilaga 2. Intervjufrågor

Frågor till branschorganisationer

Nedan finns den generella mall som följdes under intervjuer med branschorganisationer. Utöver dessa frågor så fanns det även tillfällen då ytterligare följdfrågor ställdes spontant då det var relevant.

Generellt

- Beskriv ert uppdrag
- Beskriv ditt uppdrag
- Vilka är era finansiärer?

Digitalisering

- Ser ni en stor efterfrågan inom digitalisering hos era medlemmar?
- Har ni några vanliga exempel på vad era medlemmar vill digitalisera?
- Vad erbjuder ni era medlemmar inom digitaliseringsprocessen?
- Möter detta digitaliseringsbehovet hos era medlemmar?

Cybersäkerhet

- Ser ni en ökad hotbild gällande IT-relaterad brottslighet mot era medlemmar?
- Ser ni en ökad efterfrågan om hjälp med informations- och cybersäkerhet?
    - Om ja
        - Vad efterfrågas? Varför?
        - Kan efterfrågan tillgodoses?
        - Hur gör ni det?
    - Om nej
        - Varför inte?
        - Vet ni hur ni skulle hjälpa dem om de frågade?
- Vad skulle krävas för att jobba mer med informations- och cybersäkerhet?
- Efterfrågas information/tjänster/utbildningar m.m. relaterat till cybersäkerhet från medlemmarna?

Frågor till företag

Nedan finns den generella mall som följdes under intervjuer med företag. Utöver dessa frågor så fanns det även tillfällen då ytterligare följdfrågor ställdes spontant då det var relevant.

Generellt

- Berätta vad ni jobbar med/gör
- Beskriv din tjänst

Digitalisering

- Vilka digitala lösningar använder ni på arbetsplatsen. (ex. Digitala möten kundregister, etcetera)
    - Är det något mer ni vill digitalisera? Varför har inte det digitaliserats tidigare?
        - Behöver ni hjälp med det?
    - Vet ni vart ni kan vända er för att få hjälp med era digitaliseringsfrågor?

Cybersäkerhet

- Ser ni några risker med digitaliseringen? Vilka?
    - Om ja
        - Vad gör ni för att minimera risken?
            - Om ni inte gör något, varför inte?
            - Var skulle ni vända er för att få hjälp med att minimera risken?
        - Har ni externt stöd i säkerhetstänket vid digitalisering?
        - Behöver ni mer stöd?
    - Om nej
        - Varför inte?
- Vad skulle krävas för att jobba mer med informations- och cybersäkerhet?
- Efterfrågas information/tjänster/utbildningar m.m. om cybersäkerhet från företagen?

Frågor till företagsfrämjare

Nedan finns den generella mall som följdes under intervjuer med företag. Utöver dessa frågor så fanns det även tillfällen då ytterligare följdfrågor ställdes spontant då det var relevant.

Generellt

- Beskriv ert uppdrag
- Beskriv ditt uppdrag
- Vilka är era finansiärer?

Digitalisering

- Vad erbjuder ni inom digitalisering?
    - Hur hjälper ni företag med digitalisering?
    - Möter detta alla digitaliseringsbehov hos era medlemmar?

Cybersäkerhet

- Jobbar ni med Informations- och cybersäkerhet?
    - Om ja
        - Vad efterfrågas? Varför?
        - Kan efterfrågan tillgodoses?
    - Om nej
        - Varför inte?
        - Något de planerar att göra/ något de vill göra?
- Vad skulle krävas för att jobba mer med informations- och cybersäkerhet? (kompetensutveckling, stöd, utbildning, etc.)
- Efterfrågas information/tjänster/utbildningar m.m. om cybersäkerhet från företagen?