tillväxt verket

Säker digitalisering i små och medel-stora företag

Kartläggning av behov och initiativ på marknaden

Rapport 0387

Vi stärker Sverige genom att stärka företagens konkurrenskraft

Tillväxtverket ska skapa så bra förutsättningar som möjligt för företag i hela landet att vara konkurrenskraftiga. Det innebär att vi öppnar dörrar och river barriärer – för ett Sverige där fler företag vill, kan och vågar.

Kunskap, nätverk och finansiering är våra viktigaste verktyg. Tillväxtverkets insatser skapar direkta resultat hos de företag och aktörer som vi samverkar med, men även förutsättningar för företag och regioner att möta framtidens utmaningar. Vårt största enskilda uppdrag är att bidra till att EU-medel investeras i projekt för regional konkurrenskraft och sysselsättning.

Tillväxtverkets publikationer kan laddas ner på tillvaxtverket.se.

Stockholm, december 2021
Digital: ISBN 978-91-89255-51-7
E-bok: ISBN 978-91-89255-52-4
0387

Har du frågor om denna publikation, kontakta:
Karin Östberg
Telefon, växel 08-681 91 00

Förord

Tillväxtverket arbetar för att stärka företagens konkurrenskraft. Genom kunskap, nätverk och finansiering skapar vi bättre förutsättningar för befintliga och framtida företag och attraktiva regionala miljöer där företag utvecklas.

Tillväxtverket fick 2018 regeringsuppdraget *"Höjd digital kompetens i småföretags ledningar och styrelser*". Denna studie är framtagen inom ramen för detta uppdrag och den tredje och sista i en serie om informations- och cybersäkerhet.

Uppdragets huvudsyfte är att kartlägga och analysera olika typer av initiativ och program som stöttar små och medelstora företag i arbetet att hantera informations- och cybersäkerhet. Studien gör också en genomgång av företagens efterfrågan av tjänster och rådgivning för digital säkerhet samt en sammanställning av relevanta rapporter inom området.

Kartläggningen är framtagen på uppdrag av Tillväxtverket av Unitalent AB tillsammans med Linköping Science Park och Blue Science Park. Slutsatserna är skrivna av Daniel Kullgard och Lena Miranda, Linköping Science Park. Resterande arbete har genomförts av Elias Englund Forsblom, Estelle Lohm, Niklas Andersson och Sofia Ehn.

Förhoppningen är att denna rapport ska öka kunskapen om initiativ, metoder och verktyg som kan stötta små och medelstora företags arbete för en säker digital transformation.

December 2021

Tim Brooks

Avdelningschef
Tillväxtverket

Karin Östberg

Projektledare
Tillväxtverket

Sammanfattning

Stöden till företagen är inte alltid anpassade till små och medelstora företag

Det finns ett utbud av stöd till mindre företag inom informations- och cybersäkerhet, främst utbildningar, försäkringar och olika typer av konsulttjänster. Dessutom finns kortare tester med olika frågor för företag samt olika informationsblad, guider, rekommendationer och checklistor. Utbudet riktar sig ofta till en större och bredare målgrupp. Generellt är erbjudandena utformade för större organisationer och inte specifikt utformade för SMF. Flera främjandeaktörer vill se erbjudanden som är mer målgruppsanpassade, till den aktuella branschen och till företagens specifika förutsättningar och resurser på området. Frågan är om utbudet är tillräckligt men inte når ut till småföretagen, eller om utbudet av stöd måste utökas eller erbjudas i andra format.

En del företag tvekar att satsa på cybersäkerhet och kompetensutveckling

Cyberintrång och cyberattacker blir allt vanligare i Sverige och globalt. År 2020 utsattes 80 procent av svenska bolag för minst en incident, incidenter som företagen inte alltid är medvetna om. Även om företag i stort har en hög kompetensnivå finns det risker för att en enskild medarbetare omedvetet kan skada företaget. Säkerhet bör integreras i företagens digitala utveckling redan från start och i allt förändringsarbete, för produkt- och verksamhets- och organisationsutveckling.

Informations- och cybersäkerhet är bara en av många frågor som SMF måste hantera och som resurserna ska räcka till för. En del företag med lägre digital mognad har ännu inte helt förstått vad cybersäkerhet är och varför det är viktigt. De ser ibland inte nyttan med att allt för långtgående digitalisera en verksamhet eftersom det kan innebära stora investeringar. De tvekar också att satsa på kompetensutveckling och utbildningar på grund av kostnaderna. De potentiella digitala hoten kan också göra att företag och verksamheter avstår från att investera i digitalisering.

Bland företagen finns en viss efterfrågan av anpassade utbildningar och program. Dessa bör sträcka sig över en längre tid för att företagen ska hitta rutiner och få en tillräckligt lång inkörningsperiod för sitt säkerhetsarbete. Förutsättningarna varierar dock mycket mellan företagen i olika branscher. Det kan vara svårt att ta fram ett erbjudande eller formulera ett budskap inom informations- och cybersäkerhet som fungerar för en stor och bred målgrupp av olika typer av företag.

Svårt avgöra för företagen om de beställer säkra produkter och tjänster

Mindre företag, ofta de som saknar egen IT-kompetens, har svårt att ställa rätta krav på IT- och systemleverantörer, och förstå hur säkra deras tjänster eller produkter är. De företag som levererar digitala tjänster förväntar sig dessutom att *deras* leverantörer erbjuder säkra produkter och tjänster, och att deras kunder har kompetens att beställa den säkerhetsnivå som de vill ha. 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. Köparna litar på leverantörerna.

Alla företag pekar på sina tjänsteleverantörer snett uppåt i leveranskedjan. En viktig slutsats är därför att framtida insatser också bör inkludera företagen som levererar IT-lösningar. Genom att leverera robusta och säkra digitala lösningar till alla kunder stärker leverantörsföretagen både sitt varumärke och utökar den presumtiva kundgruppen.

Innehåll

Bilagor

1 Inledning

1.1 Bakgrund

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 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.

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].

Vad gäller integrering av digital teknik ligger vi på en sjätteplats, och EU-kommissionen bedömer andra länder börjar komma i kapp på detta område. Framför allt halkar vi efter inom företagens användning av Big Data och gränsöverskridande e-handel. Det är också stor skillnad mellan olika stora företag, där små företag generellt är mycket mindre digitaliserade än de stora.[6]

Digitaliseringen är idag en grundläggande förutsättning för en ökad konkurrenskraft.[2] Med digitaliseringen ökar också sårbarheten i företagen. Företag kan utgöra målet för allvarliga cyberattacker där exempelvis system stängs ned, känslig data läcker ut, eller där elektroniska filer krypteras och lösensumma behöver betalas för att krypteringen ska hävas. Bristande kompetens inom informations- och cybersäkerhet riskerar att 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] 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.

[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

1.2 Syfte och målsättning

Syftet med rapporten är att kartlägga små och medelstora företags stödsystem och utbud för informations- och cybersäkerhet och att identifiera SMF:s nuvarande och kommande behov av stöd i arbetet för digital säkerhet. Rapporten behandlar främst de nationella stödsystemen men gör också en mindre internationell utblick.

1.3 Målgrupper

Målgrupperna i kartläggningen delas in i tre kategorier. De två första kategorierna är prioriterade för uppdraget. Övriga småföretag finns med som ett komplement för att kunna dra generella slutsatser om SMF:s efterfrågan av stöd.

- *Techföretag* – SMF som är verksamma i techbranschen och som har både nationella och internationella kunder
- *Produkt- eller tjänsteutvecklande företag* – SMF som har egen produkt- eller tjänsteutveckling av något slag
- *Övriga företag* – SMF som inte ingår i de andra två kategorierna

1.4 Avgränsning

Rapporten behandlar enbart efterfrågan som finns hos små och medelstora företag i Sverige, dvs företag med färre än 250 anställda. Vidare ligger fokus på techföretag och företag med egen produkt- eller tjänsteutveckling. Arbetet har bestått av desk research och semi-strukturerade intervjuer 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.

1.5 Metod

I arbetet används två metoder: intervjuer och en litteraturstudie genom desk research. Intervjustudien används främst för att undersöka målgruppernas behov men även för att få en uppfattning om hur målgrupperna upplever utbudet av initiativ och program som tjänster, utbildning, rådgivning, coachning och diverse digitala verktyg. Litteraturstudien syftar till att ge en överblick över informations- och cybersäkerhetsarbetet i företag och över det befintliga stödsystemet i form av initiativ och program för SMF. Den tar upp rapporter inom de tre områdena digitalisering, cyberhot och IT-, informations- och cybersäkerhet.

Intervjuer genomfördes med aktörer som tillhör någon av följande tre kategorier:

- *Företagsfrämjare*: Kategorin innefattar industrikluster, science parks, inkubatorer, organisationer och företag som arbetar för att främja utveckling och tillväxt hos företag.

- *Branschorganisationer* Kategorin innefattar branschorganisationer, dvs. arbetsgivar- och intresseföreningar för företag inom en viss bransch.

- *Företag:* Kategorin innefattar små och medelstora företag som på olika sätt berörs av cybersäkerhet.

I *bilaga 1* finns en lista över deltagarna i intervjustudien.

Intervjuerna var semistrukturerade, vilket innebär att intervjuaren följde en mall med förbestämda frågor (*se bilaga 2*) och kompletterade dem med andra, spontana frågor när det var relevant för rapportens syfte. För att kunna genomföra studien inom rimlig tid var det nödvändigt att göra ett urval bland målgrupperna. Ett antal företagsfrämjare, branschorganisationer och företag valdes därför ut, baserat på Linköping Science Parks, Blue Science Parks och Tillväxtverkets nätverk och andra aktörer genom dessa.

1.6 Metoddiskussion

Intervjustudien har en relativt stor bredd och omfattar flera branschorganisationer, företagsfrämjare och företag som är verksamma inom olika branscher. Trots bredden är ändå urvalet – framför allt för företagen – väldigt litet sett till målpopulationen. Syftet med intervjuerna är dock inte att visa exakt vad alla tycker och tänker utan i stället att ge ett djupare perspektiv på mer specifika problem. Den urvalsgrupp som används i denna rapport bör vara tillräckligt stor för att uppfylla de krav som ställs på rapporten.

För att få en bättre bild av målpopulationens åsikter, behov och kompetens gjordes även en litteraturstudie. Litteraturen utgörs av publicerat material inom valda områden.

2 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 så att den klarar krav på tillgänglighet, riktighet och konfidentialitet.[7] Med andra ord ska information alltid finnas när vi behöver den, informationen ska vara korrekt, och endast behöriga personer får ta del av informationen. *Cybersäkerhet* är 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.[8] Skyddet riktar sig mot antagonistiska hot, medan *IT-säkerhet* omfattar skydd av system mot exempelvis felbedömningar och handhavandefel.[9]

Fler cyberattacker har lett till ett större behov av kompetens inom informations- och cybersäkerhet, och företag måste numera förstå hur de kan förebygga, upptäcka och hantera cyberattacker. Några av utmaningarna är att digitala intrång inte alltid är lika direkt synliga som fysiska intrång, att medvetenheten hos de anställda kan vara låg och att det krävs resurser för att exempelvis installera skyddssystem.[10]

2.1 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 allt från överbelastningsattacker, dataintrång, cyberspionage och utpressning från enskilda hackers till statsunderstödda hacktivister. Det finns ett utbud av exempelvis konsulthjälp inom informations- och cybersäkerhet, men få erbjudanden är anpassade för SMF.[15] Många företag saknar även ekonomiska och personella resurser för att kunna möta de säkerhetsutmaningar som digitaliseringen för med sig.[11] Det är svårt att avgöra hur omfattande cyberattackerna mot svenska företag är eftersom drabbade företag ofta håller det hemligt för att inte förlora anseende.[12]

Hösten 2020 publicerade Tillväxtverket en rapport om informationssäkerhet, med uppgifter för att illustrera den digitala hotbilden. Det fanns enligt rapporten uppskattningsvis 17 000 datorer och 400 000 mobila enheter med virus eller skadliga program, och 50 procent av Sveriges företag saknade resurser för att klara en attack.[13] Det nämns vidare att de största cyberhoten mot svenska företag är omedvetna medarbetare, organiserad brottslighet och hacktivister.

---

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

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

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

[10] 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/

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

[12] 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

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

Price Waterhouse Cooper (PwC) gjorde våren 2020 en undersökning av 100 större företag, och konstaterade att allt fler svenska bolag drabbas av cyberattacker.[14] Totalt 63 procent av bolagen uppgav att de utsattes för minst en cyberattack under 2019, vilket är en ökning med 30 procent jämfört med 2018 års undersökning. Enbart 22 procent av de drabbade bolagen kunde ange kostnaden för cyberattackshanteringen. Vidare förväntas företag använda molntjänster i allt högre grad, 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 hade minskat, från 28 procent 2018 till 14 procent 2019. Få bolag verkar se cybersäkerhet som en naturlig del av ledningens och styrelsens arbete med riskhantering. En kartläggning utförd av Tillväxtverket 2019 om digitala affärsrisker anger att kompetensen inom informationssäkerhet i ledningar och styrelser är låg, men att man blir alltmer medvetna om cybersäkerhetsfrågor.[15] Dock ökar medvetenheten främst i större företag.

Inom ramen för det nationella cybersäkerhetscentret publicerades 2021 en rapport om cybersäkerhet i pandemitider, och där redovisas bland annat hur svenska verksamheter i stort agerade under delvis förändrade förutsättningar. [16] Det nämns att företagens exponering för cyberangrepp ökade när arbetsplatsen förflyttades till hemmet. 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 hade lättare att implementera nya tjänster med god säkerhet eftersom de redan inventerat och klassificerat företagets informationstillgångar. Dessa företag kunde då lättare identifiera krypteringskrav, användarbehörighetskrav och behov av autentisering. Många har lyckats väl med att hantera cybersäkerhetsutmaningarna under pandemin, men det finns risk att incidenter ännu inte har upptäckts.

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

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

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

3 Behov

Det kan verka självklart att det finns ett stort behov av olika typer av cybersäkerhetslösningar, men det blir än mer uppenbart i PwC:s rapport om cybersäkerhet i Norden. Enligt den utsattes 8 av 10 svenska bolag för minst en informationssäkerhetsincident under 2020, och vart tredje bolag uppger att de utsattes för fler än fem incidenter. Ändå bedömer PwC att det finns ett stort mörkertal. 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.[17] Myndigheten för samhällsskydd och beredskap (MSB) menar även att den pågående pandemin har inneburit nya eller förändrade hot för företagen i och med att många har fått skynda på digitaliseringen, samtidigt som de gamla hoten fortfarande finns kvar.

Det är svårt att generellt beskriva företags behov inom området cybersäkerhet eftersom det kan variera en hel del. Exempelvis skulle man kunna tänka sig att behoven ser annorlunda ut för ett företag som arbetar med stora mängder information och även arbetar digitalt i alla eller stora delar av företaget, jämfört med ett företag som inte hanterar några stora mängder information och inte heller arbetar digitalt i så hög grad.

Här beskriver vi behoven bland SMF, uppdelat i de tre kategorier, se också valen av målgrupper avsnitt 1.3.

3.1 Techföretag

Man kan tänka sig att techföretag är den kategori som har högst IT-mognad, men det gör inte att dessa företag är immuna mot cyberhot. Tvärtom visar intervjuundersökningen att techföretagens höga digitaliseringsgrad kan leda till en ökad hotbild.

Enligt intervjuerna har många techföretag ett stort säkerhetstänk med många integrerade säkerhetslösningar i sina system. Trots att man från företagens sida upplevde att systemen var säkra finns det en rädsla för att outbildad personal skulle kunna utsättas för riktade attacker, exempelvis en phishing-attack. De ser en risk för att omedveten personal råkar ge obehöriga personer tillgång till information eller viktiga delar av ett system. Detta är något som även framkommer i PwC:s rapport *Det digitaliserade Sverige – så in i Norden säkert?* [17] Flera intervjupersoner tog också upp behovet av att utbilda personal som helt saknar kompetens inom cybersäkerhet, och i många fall även generellt inom teknik.

Bland techföretagen verkar det också finnas behov av ökad kunskap och kompetens. I intervjuerna med branschorganisationerna och företagsfrämjarna framkom det att både branschorganisationer och företagsfrämjare med inriktning på techföretag upplever att många teknikföretag har en högre IT-mognad än de själva – även inom cybersäkerhet. Därför upplever branschorganisationerna och företagsfrämjarna att de inte kan bidra med någon ny kunskap eller information inom detta specifika område för denna specifika målgrupp.

Sammanfattningsvis lyftes följande behov fram:

- Fortsatt arbete med att utveckla kompetensen hos företagets samtliga anställda.

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

- Mer avancerad kunskap anpassad till de techföretag som i dag har en högre IT-mognad än de branschorganisationer och företagsfrämjare som erbjuder kurser inom cybersäkerhet.

3.2 Produkt- eller tjänsteutvecklande företag

Enligt branschorganisationer och företagsfrämjare behöver de flesta produkt- eller tjänsteutvecklande företagen mer grundläggande information om cybersäkerhet. Många av dessa företag upplevs inte vara medvetna om de risker som existerar, vilket helt enkelt leder till att de inte vet vad de behöver göra för att skydda sig mot cyberhot.

Många intervjuade företagare litar också på att deras leverantörer levererar digitala tjänster och mjukvaror som är säkra, utan att nödvändigtvis veta hur de kan kontrollera detta. Företagen behöver alltså kunna validera om de får digitala tjänster och mjukvaror som är tillräckligt säkra för det som de ska användas till.

En del företag efterfrågar utbildningar som sträcker sig över en längre period, enligt både företagen och företagsfrämjarna. Då blir det lättare att tillgodogöra sig kunskapen långsiktigt och även få in rutiner för ett systematiskt informationssäkerhetsarbete. Företagen vill också se program som går ut på att en säkerhetskunnig person under en tillräcklig period hjälper företag att sätta sig in i ett olika säkerhetsaspekter och företagsspecifika frågor.

Sammanfattningsvis lyftes följande behov fram:

- En grundläggande förståelse för vad cybersäkerhet är och varför det är viktigt.
- Förmåga att validera eller förstå säkerheten hos en digital tjänst eller mjukvara som de fått levererade av en tjänste- eller mjukvaruleverantör.
- Företagsanpassade utbildningar eller program som sträcker sig över en längre tid.

3.3 Övriga företag

I Svensk Handels rapport *Handelns utsatthet för IT-relaterad brottslighet* nämner man att bolagen inom handeln saknar kunskap om grundläggande säkerhetsfrågor och säkerhetsrutiner. Enligt Svensk Handel behövs kontinuerlig utbildning för hela företaget eftersom IT-brottsligheten ständigt förändras. I samma rapport nämns ett behov av att avstigmatisera utsattheten så att personal vågar prata om både kunskapsbrister och incidenter.[18]

Våren 2021 kom en kartläggning av digital säkerhet i jordbruket, och enligt den behöver småföretagarna bland annat mer kunskap om riskerna med digital teknik, information om säkerhetsåtgärder, information om vem som äger datasystem, samlar in och använder data. Företagarna behöver dessutom god tillgång till teknisk support när de har köpt in ny

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

teknik.[19] Småföretagen måste också snabbt få hjälp om de råkar ut för en IT-incident. Kartläggningen visar även att småföretagens digitaliseringsarbete till stor del är beroende av medarbetarnas teknikintresse, vilket generellt sett är större bland de yngre generationerna. Många lantbruksföretagare ser en utmaning i de stora initiala investeringar som krävs för att digitalisera verksamheten, samt att det är svårt att förstå om kostnaden för säkerhetslösningar motsvarar nyttan med de.

I Tillväxtverkets rapport *Digitala affärsrisker* nämns också att just de små tillväxtbolagen har svårt att se vad de har att vinna på utbildning och kompetensutveckling inom cybersäkerhet.[15] Detta lyftes även i flera intervjuer med branschorganisationerna och företagsfrämjarna, och de pekade framför allt på att små tillväxtbolag är ovilliga att lägga tid eller spendera pengar på de utbildningar som finns. Dessa bolag behöver på ett enkelt sätt kunna ta del av information om och förstå vikten av cybersäkerhet.

Sammanfattningsvis lyftes följande behov fram:

- Kontinuerlig utbildning för alla i hela företaget.
- Öppen diskussion om utsattheten vid dataintrång och IT-incidenter - utan att stigmatisera.
- Lättillgänglig information om vikten av systematiskt cybersäkerhetsarbete.

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

4 Kartläggning av utbud

I det här kapitlet redovisas utbudet av initiativ, informationsblad, utbildningar, tjänster och liknande inom informations- och cybersäkerhet som riktar sig mot små och medelstora företag. En del av utbudet har dock en större målgrupp än bara SMF. Utbudet är indelat i sju kategorier:

- initiativ
- informationsblad, rapporter och checklistor
- tester
- certifieringar och standarder
- försäkringar
- utbildningar
- konsulttjänster

Det kan finnas information eller erbjudanden som vi inte har hittat i kartläggningen, men då är det troligtvis även svårt för företagen att hitta den aktuella informationen eller erbjudandet i fråga.

4.1 Initiativ

Fyra myndigheter, i samverkan med ytterligare tre, har fått i uppdrag att inrätta ett nationellt cybersäkerhetscenter i syfte att stärka landets ”förmåga att förebygga, upptäcka, och hantera antagonistiska cyberhot mot Sverige”.[20] Centret ska bland annat underlätta informationsutbyte mellan olika aktörer inom cybersäkerhet, tillhandahålla lägesbilder om hot och sårbarheter samt ge stöd om hur verksamheter kan skydda sig mot cyberattacker. Det är även tänkt att centret ska erbjuda kompetenshöjande insatser såsom övningar och utbildningar. Centret ska byggas upp under en femårsperiod för att ge effekt 2025, så det återstår att se om och i så fall hur centret kan fungera som stöd för SMF.

För att öka kompetensen inom cybersäkerhet etablerar även RISE, Research Institutes of Sweden ett centrum för cybersäkerhet.[21] Centret kommer att finnas i Luleå och ska agera som neutral partner för industri och offentlig sektor samt 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.[22] 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.[23] Testbädden tillgängliggör test- och demomiljöer för cybersäkerhet som många mindre företag ofta saknar resurser för.

Som ett led i att oktober är EU:s informationssäkerhetsmånad genomförs i Sverige ”*Tänk säkert*”, en kampanj som riktar sig till privatpersoner och mindre företag.[24] Enligt MSB är syftet att ”öka medvetenheten om informations-och cybersäkerhetsfrågor” och att genom

---

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

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

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

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

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

konkreta tips ”kunna vidta åtgärder för ett säkrare uppkopplat liv”. Inom ramen för kampanjen anordnas bland annat webbseminarier, säkerhetstest för företagare, filmer, föreläsningar, montrar på mässor och 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.[25] Genom att erbjuda seminarier, workshoppar och evenemang är förhoppningen att man ska öka 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”.[26]

Andra koncept har även testats i Sverige. Linköping Science Park har inom ramen för Tillväxtverkets regeringsuppdrag för ”Höjd digital kompetens i små företags ledningar och styrelser” genomfört en pilotutbildning inom cybersäkerhet för SMF.[27] 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 och sätt att tidigt integrera säkerhet i både produkt- och affärsutveckling.

På hemsidan *informationssäkerhet.se* samlar olika myndigheter information som stöd för systematiskt arbete med informationssäkerhet. På sidan finns bland annat nyheter inom området, rapporter, faktafördjupningar och vägledningar samt metodstöd för att införa ett ledningssystem för informationssäkerhet. Målgruppen är de personer som ansvarar för informationssäkerhet i olika typer av organisationer.

---

[25] 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

[26] 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

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

Sammanställning av initiativ

Ansvarig aktör	Initiativ	Kategori
FRA, Försvarsmakten, MSB, Säkerhetspolisen. *Samverkan med* PTS, Polismyndigheten och FMV	Nationellt cybersäkerhetscenter	Center
	Informationssäkerhet.se	Hemsida
RISE	Centrum för cybersäkerhet	Center
	Cybernode	Nod
	Cyber range	Testbädd
MSB, Polisen m.fl.	Tänk säkert	Kampanj
LTU och Centria Yrkeshögskola	CYNIC	Projekt
Linköping Science Park	Pilotutbildning inom cybersäkerhet	Projekt
MSB	Metodstöd för systematiskt informationssäkerhetsarbete	Praktiskt stöd och verktyg

4.2 Informationsblad, rapporter och checklistor

I vägledningen *Informationssäkerhet för små företag* ger MSB rekommendationer för företag med upp till tio anställda om hur de kan förbättra informationssäkerheten i företaget.[28] Den innehåller praktiska tips på hur information ska skyddas samt vad man ska göras ifall företaget råkat ut för någon vanlig cyberincident. Den behandlar bland annat virusskydd, säkerhetsuppdateringar, molntjänster, utpressning och skydd av trådlöst nätverk. Det redovisas även steg-för-steg-åtgärder mot fyra sorters bedrägerier – id-kapning, utpressningsvirus, företagskapning och fakturabedrägeri.

Säkerhetspolisen rekommenderar i sin rapport *Vägledning i säkerhetsskydd. Informationssäkerhet* säkerhetsåtgärder för verksamheter samt hur de kan förhålla sig till informationssäkerhet i stort.[29] Viss förkunskap kan krävas för att ta till sig innehållet i vägledningen. Den ger dock vägledning om bland annat hantering av säkerhetskänsliga uppgifter, informationssystems arkitektur, incidenthantering och kontroll av åtkomst och behörigheter.

Inom ramen för det nationella centret för cybersäkerhet publicerades rapporten *Cybersäkerhet i Sverige 2020 – rekommenderade säkerhetsåtgärder,* med åtgärder för en

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

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

säker IT-miljö.[30] Rekommendationerna ska vara ett stöd i prioriteringar i säkerhetsarbetet, och ska alltså inte ersätta ett systematiskt säkerhetsarbete. De täcker exempelvis säkerhetsuppdateringar, säkerhetskopior, behörighets- och autentiseringsfunktioner, segmentering av nätverk och förmåga att upptäcka säkerhetshändelser. Innehållet vänder sig till medarbetare som är ansvariga för IT-miljön. Målgruppen är primärt myndigheter, kommuner och regioner men rekommendationerna kan också användas av målgruppen SMF. Vidare har MSB och Polisen i samverkan gett ut ett informationsblad med checklistor som kan användas av företag för att förbättra säkerheten.[31] Checklistorna gäller bland annat skydd mot skadlig kod och skydd mot att obehöriga får tillgång till värdefull information.

Stöldskyddsföreningen (SSF) erbjuder guider inom grundläggande cybersäkerhet.[32] Sex områden berörs, exempelvis skydd av nätverk, kontroll av behörigheter och informationssäkerhet vid upphandling av IT-relaterade tjänster. SSF erbjuder även en guide om att förebygga bedrägerier, exempelvis ransomware och bluffakturor.[33] Under 2020 publicerades även en guide om företagsbedrägerier, med fokus på hur företag kan skydda sig mot ökningen av bedrägerier i kölvattnet på coronapandemin.

Många företag som erbjuder tjänster inom IT-, informations- och cybersäkerhet har guider med grundläggande steg mot en säker IT-miljö som SMF kan ta del av. Exempel är Cygate (Telia)[34], Advenica[35] och Conscia[36]. Det finns även rapporter och guider som föreningar och organisationer har gett ut, exempelvis Säkerhetsbranschens broschyr om cybersäkerhet och informationssäkerhet med fokus på kamera[37], Teknikföretagens guide till medvetet säkerhetsarbete i mindre teknikföretag[38] och Internetstiftelsens guide #29 om internets baksida och hur företagare kan skydda sin verksamhet[39].

---

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

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

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

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

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

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

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

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

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

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

Sammanställning av informationsblad, vägledningar, rapporter, och checklistor

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

		• Bluffakturor

4.3 Tester

MSB och SSF Stöldskyddsföreningen har tillsammans skapat ett självtest för företag som ger en indikation om hur bra IT-säkerhet de har.[40] Det finns även ett säkerhetstest framtaget för företagsportalen *verksamt.se* som går igenom digitala risker som företagare behöver känna till, exempelvis skydd av information och sätt att undvika bedrägerier.[41]

En del konsultföretag med tjänster inom IT-, informations- och cybersäkerhet erbjuder också självtester på sina hemsidor. Exempelvis har If en kort test inom IT-säkerhet för företagsanställda,[42] följt av 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.[43]

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 (tar ungefär tio minuter per område att genomföra)
Verksamt.se	• Skydd av information • Bedrägerier	Åtta frågor
If	IT-säkerhet	Tio frågor
Cygate	Cybersäkerhet	Uppgift saknas
Advenica	Utvärdering av företagets säkerhet	Sju frågor

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

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

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

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

4.4 Certifieringar och standarder

Svensk Brand- och Säkerhetscertifiering (SBSC) erbjuder en certifiering inom cybersäkerhet kallad SSF 1101 Cybersäkerhet BAS.[44] Normen för certifieringen har tagits fram av SSF i ett samarbete mellan Polisen, MSB och branschorganisationer, och den anger grundläggande IT-säkerhetskrav för SMF. Certifikatet är giltigt i tre år. SSF 1100 Certifierad Informationssäkerhetskonsult (CISK) riktar sig i stället till personer med kompetens inom IT- och informationssäkerhet och vägleder företag i att införa säkerhetsåtgärder enligt SSF 1101.[45]

ISO 27000-serien består av olika standarder inom informations- och cybersäkerhet samt dataskydd och kan ”tillämpas inom alla organisationer oavsett bransch, storlek och verksamhet”.[46] Serien stödjer bland annat införande av säkerhetsåtgärder för att skydda information. Företag kan certifiera sig mot ISO/IEC 27001. MSB har metodstöd som bygger på denna standard.

Common Criteria for Information Technology Security Evaluation (CC) är en standard för att utvärdera säkerheten hos IT-produkter,[47] 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

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

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

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

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

4.5 Försäkringar

Det finns ett antal försäkringar som är gjorda för att stödja företagare vid cyberbrott. De flesta försäkringarna omfattar bland annat utredning av intrånget och stöd för att komma i gång igen, ersättning för förlorad inkomst när verksamheten står stilla och stöd vid betalning av skadestånd. 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

4.6 Utbildningar

Det finns ett antal utbildningar inom informations- och cybersäkerhet. Tabellen nedan listar ett urval. Enbart en är uttalat riktad mot SMF, och därför behöver företagen själva veta vilka utbildningar som är relevanta för dem.

Utöver de listade utbildningsanordnarna nedan finns det flera företag, exempelvis Secure State Cyber och Nimblr, med olika erbjudanden. Det saknas dock tillgänglig information om utbildningarnas innehåll och omfång

Universitet och högskolor erbjuder också kurser för privatpersoner, med olika förkunskaps- och antagningskrav.

Sammanställning av utbildningar

Utgivare	Namn	Pris (kronor)	Omfång	Målgrupp
SSF	Cybersäkerhet – Bas Utbildning	9 500	1 dag	SMF
	Säkerhet bas – Utbildning	16 300	2 dagar	Chefer och anställda som jobbar med säkerhetsfrågor
MSB	Digital informationssäkerhets-utbildning för alla (DISA)	Gratis	Materialet finns online. Deltagarna arbetar i egen takt	Alla inkl. SMF
	Grundkurs i säkerhet i industriella informations- och styrsystem	Gratis	2 dagar	Utvecklingsingenjörer och operatörer inom information och styrsystem
	Informationssäkerhet - Operativ informationssäkerhets-kurs	Gratis	2–3 minuter i veckan i 14 veckor	Personal som arbetar med säkerhetsfrågor *OFFENTLIG SEKTOR*
	Informationssäkerhet - Taktisk informationssäkerhets-kurs	Gratis	5 minuter i veckan i 13 veckor	CISO *OFFENTLIG SEKTOR*
	Kurs i strategisk och systematisk informationssäkerhet	Initialt viss avgift	3 eller 6 dagar	Chefer och CISO *OFFENTLIG SEKTOR*
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

CISO = *Chief Information Security Officer*.

4.7 Konsulttjänster

Det finns många konsultföretag som erbjuder tjänster inom IT-, informations- och cybersäkerhet, men alla är inte relevanta för SMF. Tabellen visar vilka som erbjuder konsulttjänster till SMF, med ett urval av deras tjänster.

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 och säkerhetsgranskning.
Cybercom	Penetrationstester, molnsäkerhet och sårbarhetsskanning.
IT-Total	Bedömning och test av nuvarande IT-system, rådgivning och experthjälp vid misstanke om intrång och cyberattack.
Knowit	Helhetsleverantör inom cybersäkerhet och relaterad juridik.
Outpost24	Säkerhetstest av applikationer och DevOps samt nätverkssäkerhet och molnsäkerhet.
Rote Consulting AB	Säker och effektiv informationshantering.
Secify	Risk- och sårbarhetsanalys, riskcheck och penetrationstester.
Truesec	Kodgranskning, penetrationstester och utvärderingar av phishing-risk.
Yes it networking solution	IT-säkerhetstjänster, coachning och GDPR.
Weop	Analyser av och utbildning inom informationssäkerhet.
West code solutions	Rådgivning.

4.8 Internationell utblick

Nedan görs en kort genomgång av några internationella initiativ för informations- och cybersäkerhet.

Stöd till svenska SMF

Svenska SMF kan 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 om hur man kan säkra sitt företag.[48] Rapporten är uppdelad i tre delar: grundläggande, mer djupgående och organisatorisk. Råden är djupgående även i den grundläggande delen men inte lika konkreta som råden i MSB:s vägledning *Informationssäkerhet för små företag*.

Ett annat exempel på internationellt stöd är en checklista utgiven av Financial Industry Regulatory Authority (FINRA) för att hjälpa små företag att bli säkrare.[49] Checklistan är baserad på FINRA:s rapport om arbete inom cybersäkerhet och på National Institute of Standards and Technologys (NIST:s) ramverk för cybersäkerhet. Det EU-finansierade initiativet *Digital SkillUp* erbjuder också stöd till SMF i form av bland annat onlineutbildningar (där cybersäkerhet är ett av tre fokusområden), med syftet att SMF ska lära sig mer om ny teknik och höja sin digitala mognad.[50]

Stöd till SMF i andra länder

Flera av Sveriges grannländer har också branschföreningar som samlar cybersäkerhetsindustrin, däribland InfoBalt i Litauen och FISC i Finland. Även TeleTrust i Tyskland och CenSec i Danmark har liknande roller, men arbetar inte bara med cybersäkerhet. I Litauen är det försvarsdepartementet, Litauen Ministry of Defence, som äger frågan som helhet, och som erbjuder information, guider och utbildningar. Det är enskilda privata bolag som tillhandahåller själva tjänsterna. I Norge finns NorSIS, en del av regeringens satsning på informationssäkerhet, som tillhandahåller aktiviteter inom området åt privat och offentlig sektor. Det finns även en satsning för att få ungdomar och lärare mer intresserade av cybersäkerhet – projektet Cybersmart som verkar för en bättre digital säkerhetskultur.

Enligt nätverket International Association of Science Parks and Areas of Innovation (IASP) finns en science park i Spanien som erbjuder rådgivning till SMF om cybersäkerhet, exempelvis om hur man gör backup, hur lösenord hanteras på ett säkert sätt och hur internet och e-post kan användas säkert.

I Nederländerna finns ett ”Digital Trust Center”, initierat av Ministry of Economic Affairs and Climate Policy och Ministry of Justice and Security, som har två huvudsyften. Det första är att erbjuda företag oberoende information om digitala sårbarheter och konkreta förslag på åtgärder för att minska den digitala sårbarheten samt att agera som en digital plattform som uppfyller detta syfte. Det andra huvudsyftet är att främja

---

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

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

[50] 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/

cybersäkerhetsallianser mellan företag. Digital Trust Center har flera erbjudanden till både små och stora företag, bland annat tillgång till deras digitala plattform med aktuell och trovärdig information. Denna information består bland annat av grundläggande riktlinjer som ska finnas till stöd för företagens arbete med cybersäkerhet, uppdaterad information om aktuella hotbilder och lämpligt agerande om man drabbas samt steg-för-steg-guider för hur företag ska upptäcka om de blivit angripna. Digital Trust Center erbjuder även bidragssystem till företag som vill samarbeta med andra företag om cybersäkerhetfrågor.

4.9 Summering av utbud

Kartläggningen synliggör att SMF kan få vissa stöd inom informations- och cybersäkerhet, både kunskapshöjande och rådgivande stöd i form av bland annat guider, tester, försäkringar, utbildningar och konsulttjänster. Däremot kan företagen ha svårt att lägga tillräckligt med resurser på området. En del hjälpmedel är mer passiva, såsom digitala guider och tester, men det krävs ändå ett visst engagemang för att företagen ska hitta dessa. En del av utbudet som presenterats i kartläggningen riktar sig mot en större målgrupp, exempelvis organisationer i stort, så utbudet är inte specifikt anpassat för SMF. Frågan är om utbudet är tillräckligt men inte når ut till småföretagen, eller om utbudet av stöd måste utökas eller erbjudas i andra format.

5 Diskussion

5.1 Upplevda glapp mellan utbud och behov

Techföretagen behöver arbeta vidare med att kompetensutveckla alla sina medarbetare för att mindre säkerhetsutbildad personal inte ska bli svaga länkar och mål för phishing-attacker. De små tillväxtbolagen – till viss del också techföretagen – behöver snarare förstå varför cybersäkerhet överhuvudtaget är nödvändigt. Flera företagsfrämjare och branschorganisationer menar att det finns sådana utbildningar, medan andra menar att utbudet saknas på grund av bristande intresse och efterfrågan från små tillväxtbolag alternativt bristande kunskap hos företagsfrämjaren. Samtidigt säger företagen i intervjuer att de är intresserade av att öka medvetenheten och kunskapen men att utbudet antingen inte existerar, eller att kostnaderna är för höga. Genomgången i avsnitt 4.6 visar att det finns utbildningar inom detta ämne, så frågan är varför behovet kvarstår. Det kan behövas ytterligare undersökningar för att se om det beror på att utbudet är för begränsat, om utbildningarna inte tillräckligt anpassade för SMF eller om de bedöms vara för dyra.

5.2 Brist på beställarkompetens

Kapitel 3 visar att produkt- eller tjänsteutvecklande företag behöver kunna validera eller förstå hur säker en digital tjänst eller mjukvara är som de fått levererade av en leverantör. En intervjuperson tog också upp att detta är svårt vid förhandlingar med leverantörer. Man upplever att man kan bli ”bortgjord” av säljare och har svårt att bedöma huruvida något är så säkert som de säger eller om det enbart är ett säljknep. En del SMF som beställer digitala tjänster får helt enkelt förlita sig på att tjänsterna som de köper är säkra. Samtidigt menar leverantörer av säkerhetstjänster att de som beställer en IT-tjänst inte kan förvänta sig att säkerheten kommer med, om de inte har ställt tillräckliga krav på detta. Det finns alltså risk för att säkerhetsfrågan i dessa fall hamnar mellan stolarna, vilket kan resultera i bristande säkerhet.

Många IT-produkter och digitala 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.

6 Slutsatser

Sverige är ett av EU:s mest digitaliserade länder, men digitaliseringen innebär både möjligheter och risker. Samtidigt är säkerhetsfrågan sällan prioriterad i insatser för att öka digitaliseringen. Arbetet med just informations- och cybersäkerhet för SMF kan därför bli en stor utmaning.

6.1 Digital säkerhet är komplex

Frågan om cybersäkerhet är stor och komplex. Hotbilden omfattar allt från samordnade och systematiska attacker från stater till ett sätt för kriminella att tillskansa sig medel. Även konsekvenserna av bristande förmåga att hantera olika typer av cyberhot är komplexa, med exempelvis påverkan på samhällsfunktioner såsom el- eller matförsörjning, kommunikationer eller betalsystem. Andra störningar driver kostnader för bolagen. En annan komplexitet är att frågan rör hela organisationen, så att varje individ potentiellt är den svagaste länken.

Ur ett nationellt offentligt perspektiv jobbar verksamheter som MSB, Säkerhetspolisen, Polismyndigheten och Militära underrättelse- och säkerhetstjänsten för att informera och utbilda i frågan ur ett samhällsperspektiv. Ur ett näringslivsperspektiv arbetar bland annat Tillväxtverket för att främja digitalisering med fokus på tillväxt och innovation i små och medelstora företag.

Vi ser allt fler intrång och hackerattacker både i Sverige och globalt och att dessa händelser får ett allt större mediegenomslag. Det stora mediefokuset på cyberhot kan påverka företag negativt. Det blir ett slags ”moment 22” kring frågan, där företag och verksamheter kan avstå från digitalisering på grund av alla potentiella hot och risker som en ökad uppkoppling medför, vilket i sin tur skulle kunna bidra till en minskad tillväxt och minskad innovation. Det är därför viktigt att säkerhet integreras i all digital utveckling redan från starten och som en integrerad del i företagens förändrings- och affärstrategiarbete, i produkt- och tjänsteutveckling. Säkerhetsfrågorna bör i större utsträckning hanteras på styrelse-, lednings- och ägarnivå också i de mindre bolagen.

6.2 Kompetensen och kunskapen finns delvis på marknaden – men den är inte tillräckligt anpassad för SMF

Det finns flera parallella nationella cybersäkerhetsinitiativ, men dess verksamheter når idag i mindre utsträckning målgruppen små och medelstora företag. Kunskapen finns, men den behöver vidareutvecklas, ytterligare tillgängliggöras och paketeras för att nå och passa SMF:s behov. Myndigheter, forskningsinstitut och branschorganisationer kan ha svårt att tillgodose alla behov. Företagsfrämjare behöver därför utbildas för att bära med sig säkerhetsperspektiven när de ger råd och stöd till SMF.

Det kan också vara svårt att rikta *ett* budskap inom informations- och cybersäkerhet till en för bred målgrupp. Förutsättningarna varierar mellan branscher, men även mellan olika företag. Organisation, tillväxtfas och kultur påverkar hur företag arbetar med säkerhetsfrågorna. Informations- och cybersäkerhet är dessutom bara en av de frågor som dagens SMF måste hantera för sin verksamhets- och affärsutveckling. Andra prioriterade frågor handlar inte minst om hållbarhet, kompetensförsörjning och internationalisering.

Det finns också en övertro på att exempelvis checklistor och guider ska lösa informationsbehovet för en så viktig fråga. Satsningar behöver stötta relevanta främjandeaktörer som kan stärka 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. Stödet till små och medelstora företag bör nivå- och målgruppsanpassas för att möta behov både kortsiktigt och på längre sikt. Företagen kan ha en lång inkörningstid eftersom säkerhetsområdet är nytt för många. För att stödsystemets aktörer ska fylla sin funktion även i framtiden är det viktigt att insatserna kontinuerligt ses över och anpassas utifrån SMF:s behov och de digitala hoten.

6.3 Var ska satsningen ske?

Rapporten visar att leverantörerna av olika system- och IT-lösningar har ett stort ansvar för att leverera så säkra produkter och tjänster som möjligt. Alla bolag pekar på sina leverantörer: Det lilla bolaget utgår från att leverantören säljer säkra produkter, och denna leverantör utgår i sin tur från att dess leverantör gör det, och så vidare. Många leverantörer tycker även att det behövs bättre beställarkompetens. En slutsats är därför att insatser också bör inkludera företagen som levererar IT-lösningar. Blir de bättre på att hantera säkerhet för sina kunder minskar även risken för kunderna. Genom att leverera robusta och säkra digitala lösningar till alla kunder stärker leverantörsföretagen både sitt varumärke och utökar den presumtiva kundgruppen.

Insatser bör även riktas till ledning och styrelser i små och medelstora företag. Företagen behöver stöd och rådgivning för att förstå hur de strategiskt kan digitalisera sin verksamhet på ett säkert sätt och vilka kostnader och utvecklingsinsatser som krävs.

6.4 Kunskapshöjande insatser

SMF behöver utbildning och mer kunskap, och behovet finns inom flera typer av företag och branscher. För att möta det behovet behövs en struktur som framgångsrikt kan nå ut med erbjudanden. Denna fråga är därför starkt sammankopplad med frågan om regionala kontaktpunkter för cybersäkerhet, s.k. regionala cybersäkerhetscentrum. Att ta fram utbildningar som finns tillgängliga hos olika aktörer, exempelvis på nätet, är möjligen inte det mest framgångsrika. I stället föreslår vi att kompetenshöjande insatser har fokus på aktualitet, relevans och incitament.

Cybersäkerhetsområdet utvecklas i en rasande takt, och det är svårt att förutsäga vad som är morgondagens hot i olika branscher. Utbildningar inom cybersäkerhet måste med andra ord vara väldigt dynamiska och erbjudas i nära samverkan med industrin för att vara aktuella. Dessutom måste de vara relevanta för målgruppen i fråga, så att mottagarna har rätt förkunskaper inom området och utbildningen är anpassad till deras egen kontext. Det bör även finnas incitamentsmodeller som gör att målgruppen får fördelar, eller undviker nackdelar, om de tar del av kompetensutveckling.

6.5 Övrigt

Varje år genomför MSB och ett antal samarbetspartner kampanjen ”*Tänk säkert*”, för att öka medvetenheten om informations- och cybersäkerhetsfrågor och i förlängningen skapa en större öppenhet i frågorna. Vi vill gärna se både fler och större initiativ för att öka just

medvetenheten om informations- och cybersäkerhet och för att anställda ska våga berätta om de blivit utsatta eller råkat göra ett misstag.

Genom en ökad medvetenhet bör ämnet också bli mer intressant och attraktivt att arbeta med, vilket är viktigt för att frågan ska prioriteras hos företagen. En ökad medvetenhet om de *certifieringar* som finns skulle även göra det lättare för SMF att hitta rätt typ av leverantörer som är säkra och ge stöd i vilka krav som kan ställas.

I Tillväxtverkets rapport *Informationssäkerhet. Små och medelstora företags förmåga att digitalisera och växa i en värld där informations- och cybersäkerhet blir allt viktigare* finns många bra förslag på kompetenshöjande insatser. Några av dem ser vi som värda att undersöka närmare: att ta fram konkreta ”roadmaps” med vägledning, att anpassa ramverk såsom NIST och CIS så de kan användas av SMF och att erbjuda konsultcheckar för strategiskt informationssäkerhetsarbete.

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?

Tillväxtverket
Swedish Agency for Economic
and Regional Growth
Tel 08-681 91 00
tillvaxtverket.se

Tillväxtverket arbetar för hållbar tillväxt och konkurrenskraftiga företag i alla delar av Sverige. Det gör vi genom att stärka företag och regioner. Vi erbjuder kunskap, nätverk och finansiering. Det ger direkt nytta till företag, och också förutsättningar för företag och regioner att möta framtidens utmaningar. Tillväxtverket är en nationell myndighet med regional närvaro på nio orter. Ett Sverige med fler företag som vill, kan och vågar är vår vision.

tillväxt
verket