Kartläggning av allmänhetens och mindre företags behov av stöd för ökad informations- och cybersäkerhet.

Förstudie till SSF initiativ Nationellt Nav

2024-01-31

En förstudie som tagits fram av SSF med stöd av MSB.

Kontaktperson: Per Klingvall, SSF
per.klingvall@stoldskyddsforeningen.

SSF
Stöldskyddsföreningen

1. Innehållsförteckning

2. Sammanfattning

Förstudien är en kartläggning av allmänhetens och mindre företags behov avseende förbättrad informationshantering och cybersäkerhet. Inom denna ram ingår att definiera och segmentera målgrupperna i syfte att identifiera vilka åtgärder inom vilka områden som olika målgrupper är i behov av. Projektet innebär ett första steg mot ett långsiktigt arbete att ta fram en samlingsplats, här benämnt *nationellt nav*, dit allmänhet och mindre företag med begränsade it-säkerhetsresurser kan vända sig.

För att besvara centrala frågor om målgrupperna kring segmentering, behovsanalys och prioritering har existerande undersökningar från perioden 2020 till 2023 använts. Syftet är att öka förståelsen för målgruppernas förhållande till informations- och cybersäkerhet, inklusive deras vidtagna säkerhetsåtgärder, oro och grad av utsatthet för bedrägerier och brott.

Förstudiens material fokuserar till stor del på att särskilt undersöka förhållanden kring digitala brott. Förmågan att hantera risker och att skydda sig mot digitala brott bidrar även till en stärkt förmåga inom informations- och cybersäkerhetsområdet som helhet.

Kartläggningen presenteras genom indexvariabler som skapats utifrån respondenternas egen gradering av oro, vidtagna säkerhetsåtgärder och utsatthet i digitala miljöer. De index som presenteras i förstudien är *orosindex* (oro för risker och för att själv drabbas), *robusthetsindex* (hur medveten man är för faror och egna vidtagna säkerhetsåtgärder), *utsatthetsindex* (självskattad utsatthet för *försök* till brott) och *brottsindex* (självskattad utsatthet för *faktiska* brott). Ytterligare ett index har skapats för målgruppen allmänhet, *motivationsindex* (hur intresserad man är av att söka hjälp och kunskap för att lära sig mer).

Kartläggningen visar att finns ett generellt behov av ökad informations- och cybersäkerhet hos både allmänheten och mindre företag. För att forma en effektiv framtida nationell strategi bör framtida prioritering av insatser anpassas utifrån kritiska områden som på sikt bidrar till beteendeförändringar som att exempelvis höja miniminivån av säkerhet hos de mest sårbara segmenten, utveckla mer robusta segment att höja den egna kunskapsnivån ytterligare eller att få de motiverade att bidra med kunskapsspridning till fler. Särskild uppmärksamhet behövs för segment med lägre robusthet, såsom kvinnor, åldersgruppen 64+ och 16–25 år, lågutbildade, mindre företag med 0–99 anställda samt branscher inom handeln, transport, hotell och restaurang. Segment som kräver andra typer av insatser är män, höginkomsttagare, 26–45 åringar samt företag med 100–249 anställda och tjänstesektorn, som alla utmärker sig för högre robusthet och högre utsatthet.

Förstudiens slutsats är att det nuvarande nationella stödet inom informations- och cybersäkerhet bör utökas för att öka medvetenhet om digitala risker och öka kunskapen om hur man skyddar sig. Detta är avgörande för att snabbt stärka allmänhetens och mindre företags egna säkerhetsåtgärder och därigenom göra hela Sverige säkrare. Som ett nästa steg föreslås därför att aktiviteter riktas mot prioriterade segment för att se hur engagemang och villighet till förändrade beteenden kan ökas.

Försvarsberedningen har i sin rapport Kraftsamling från 19 december 2023 pekat på förstudiens roll som första steg för framför allt företag. Den här förstudien lägger den grunden.

3. Inledning

I en förändrad omvärld med fortsatt digitalisering av samhället, utveckling av nya teknologier, geopolitiska spänningar, antagonistiska hot och påverkansoperationer, utmanas säkerheten och behovet av trygghet i Sverige växer. Nya regulatoriska krav på informations- och cybersäkerhet ska hantera dessa osäkerheter, men de faller inte ut över hela samhället då kraven främst ställs på aktörer som definieras som samhällsviktiga. På den dagliga medieagendan talas det om att allmänheten och mindre företag är dåligt rustade mot cyberattacker och bedrägerier. För få människor i Sverige genomför åtgärder för att minska sin digitala sårbarhet [1]. Samtidigt är även svenska företag enkla offer för digitala brott på grund av Sveriges höga digitalisering, men låga informations- och cybersäkerhet[2]. För att minska dessa målgruppers sårbarhet och öka skyddet mot digitala brott har förstudien i uppgift att kartlägga allmänhetens och de mindre företagens behov av insatser för ökad informations- och cybersäkerhet, vilka stöd som finns idag inom området samt om de bedöms vara tillräckliga. I arbetet ingår även att segmentera målgrupperna i syfte att identifiera vilka åtgärder inom vilka områden som olika målgrupper är i behov av.

3.1. Frågeställningar

Förstudien ska undersöka allmänhetens samt mindre företags behov av åtgärder avseende förbättrad informations- och cybersäkerhet samt vilka behov av stöd/hjälp de har för att öka det egna skyddet.

- Definiera och segmentera målgrupper.
- Identifiera vilka behov som finns hos allmänhet och mikroföretag avseende förbättrad informationshantering, informationssäkerhet och cybersäkerhet.
- Baserat på behovsanalysen, ta fram ett förslag på vilken eller vilka segment av målgrupperna som ska prioriteras inom vilka områden i det framtida arbetet.
- Beskriv gapet mellan målgruppernas behov och nuvarande stöd inom informations- och cybersäkerhetsområdet.

3.2. Förstudiens hypotes

Förstudiens hypotes är att den grundläggande informations- och cybersäkerheten hos målgrupperna allmänhet och mindre företag inte är på en tillräckligt hög nivå, och att det finns en klyfta mellan målgruppernas behov av hjälp inom informations- och cybersäkerhet och det nationella utbud som erbjuds dessa grupper.

3.3. Omfattning och avgränsning

Förstudien omfattar kartläggning av målgrupper och segment via befintliga sekundärdata, varav några frågeområden har kompletterats med nya undersökningar och enkätfrågor under hösten 2023. Målgrupper som kartlagts är allmänhet samt företag med 0–249 anställda. Syftet med att undersöka en bredare

1 https://www.pwc.se/sv/pressrum/cyberhot.html

2 https://stockholmshandelskammare.se/rapporter/rapport-cyberbrott-mot-svenska-foretag/

företagsmålgrupp än projektdirektivet föreslår, vilket är mikroföretag (0-9 anställda), är för att identifiera och förstå skillnader mellan mikroföretag och något större företag och utifrån det dra slutsatser.

Förstudien beskriver även översiktligt aktörer i Sverige som bedriver verksamhet för målgrupperna inom informations- och cybersäkerhetsområdet.

En framtida avgränsning i en nationell samlingsplats kan komma att göras gentemot företag som klassas som samhällsviktiga utifrån MSB:s definition[3]. Dessa företag omfattas, eller kan komma att omfattas, av lagar som hanterar frågor kring informations- och cybersäkerhet vilket kommer styra deras hantering av den grundläggande säkerheten.

Förstudien fokuserar på informations- och cybersäkerhet i kontexten skydd mot digitala brott och är därmed till största del avgränsad till kriminella och antagonistiska hotkällor och risker. Förstudien utgår därför inte från ett allriskperspektiv, där även områden som exempelvis hård- och mjukvarufel, bristande styrning och naturrelaterade hot ingår. Notera att behovsanalysen inte svarar på *hur* förändringar hos målgrupperna ska åstadkommas, utan det är en fråga i ett nästa steg efter förstudien.

3.4. Definitioner

För definitioner av begrepp inom informations- och cybersäkerhet hänvisas till MSB:s termbank[4]. Övriga begrepp som används i förstudien definieras här:

Digitala brott: Enligt SSF:s definition är det ett brott som sker i den digitala miljön, främst bedrägerier och dataintrång.

Grundläggande cybersäkerhet: Begreppet syftar enligt SSF:s definition till målgruppens behov av åtgärder för att skapa och behålla en grundläggande nivå av informations- och cybersäkerhet, med fokus på skydd mot digitala brott. Omfattar både förebyggande åtgärder och åtgärder för att hantera en incident. Se bilaga 1.

Mindre företag: Med mindre företag avses i förstudien alla företag med upp till 249 anställda. EU:s indelning av företagsstorlek utifrån medelstora, små och mikroföretag har inte kunnat användas i förstudien på grund av att företagsindelningarna i sekundärdata skiljer sig åt. Det är även intressant att studera skillnaderna mellan olika företagsstorlekar, därav valet.

Segment: Med segment avses en mindre grupp i målgruppen som har gemensamma särdrag som exempelvis ålder, kön och utbildning hos allmänheten, samt antal anställda eller digital mognad hos företag.

Index: Index är ett sammanfattande mått som består av flera olika komponenter, vilket används för att reducera data för att underlätta analys och resultat.

3 https://www.msb.se/contentassets/d8fca23b124c4686a629970fd2c1aa31/vagledning-for-identifiering-av-samhallsviktig-verksamhet-msb1408---juni-2019.pdf
4 https://termbanken.informationssakerhet.se/

4. Nulägesanalys

4.1. Informations- och cybersäkerhet bland företag och allmänhet

Den digitala transformationen ökar mindre företags exponering för digitala säkerhetsrisker. Pandemin gjorde allt fler företag beroende av digital teknik, vilket illasinnade aktörer kan utnyttja genom att intensifiera cyberattacker. Mindre företag har ofta sämre förmåga att hantera de digitala säkerhetsriskerna, då de tenderar att sakna kunskap och resurser för att upprätthålla en grundläggande cybersäkerhet. Mindre företag behöver inkludera informations- och cybersäkerhet och relevanta åtgärder i verksamheten på ett mer omfattande vis än som görs idag, för att minska risken för egen del samt för andra i ekosystemet. [5]

Ett alltmer digitalt och uppkopplat samhälle leder till en bekvämare vardag, men även till ökad risk för utsatthet. När tekniken blir allt säkrare utvecklar kriminella och antagonister sina tillvägagångssätt och vänder sig direkt mot potentiella brottsoffer för att på den vägen komma förbi tekniska skyddsmurar. Utvecklingen driver på ett fortsatt stort behov av medvetna och säkra internetanvändare.[6]

4.2. Nationellt utbud av stöd och hjälp inom informations- och cybersäkerhet

Det finns idag flera aktörer som erbjuder hjälp och stöd inom informations- och cybersäkerhet till olika målgrupper i Sverige. Bland annat myndigheter, säkerhetsföretag, konsultbolag, organisationer, forum, stiftelser och föreningar.

De statliga myndigheterna ger stöd i form av kostnadsfri kunskap och aktiviteter till organisationer och företag, men det finns en risk att mindre aktörer inte kan dra nytta av dessa stöd på grund av avsaknad av resurser, kompetens eller organisering som krävs.

Det finns en rad olika privata aktörer som erbjuder stöd och hjälp till näringslivet. Men utbudet är sällan kostnadsfritt och mindre företag med begränsade resurser har mindre möjligheter att ta del av kommersiella erbjudande. Kostnadsfria stöd till företag är sällan anpassade för mindre företags verksamheter, istället återspeglar de vanligtvis större organisationers vardag och resurser. Det finns ett fåtal tjänster som erbjuder personlig hjälp till mindre företag, men de flesta av dessa tjänster är inte kostnadsfria.

För allmänheten finns det till viss del ett utbud av hjälp och stöd i form av kostnadsfri information, produkter, utbildning och hjälp. Dock är det svårt för allmänheten att hitta en samlad plats med hjälp och stöd, samt veta exakt vilka åtgärder man bör vidta för att upprätthålla den grundläggande cybersäkerheten. Förutom SSF Stöldskyddsföreningens plattform Säkerhetskollen.se finns inte heller någon samlad plats dit allmänheten kan vända sig för att få personlig och kostnadsfri hjälp inom området.

I förstudiens bilaga 3 ges exempel på vilka organisationer som idag ger stöd inom området, vilken typ av stöd som ges samt vilka målgrupper som de olika organisationer vänder sig till.

---

5 https://www.oecd-ilibrary.org/industry-and-services/the-digital-transformation-of-smes_71cb507b-en

6 https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/sammanfattning/

5. Metod och material

För att kunna besvara förstudiens frågor har en undersökning och kartläggning av målgruppernas nuläge inom informations- och cybersäkerhet, utifrån perspektivet digitala brott, genomförts. Analysen har utförts på sekundärdata.

5.1. Material

Datainsamlingen har gjorts från befintliga undersökningar som ger svar på allmänhetens och mindre företags självrapporterade oro, kunskap, åtgärder och utsatthet utifrån perspektivet informations- och cybersäkerhet med fokus på digitala brott.

Data om allmänheten har hämtats från undersökningar framtagna av Internetstiftelsen, MSB och Stöldskyddsföreningen under perioden 2020 till 2023, se bilaga 6.

Data om företag har hämtats från undersökningar framtagna av Företagarna, Telia och Telenor under perioden 2022 till 2023, se bilaga 6. Telenors undersökning är baserad på företag upp till 249 anställda, medan Telias och Företagarnas undersökningar speglar alla företag i Sverige oavsett storlek. Det bör tilläggas att andelen företag med 0–249 anställda i Sverige utgör 99,9 % av samtliga företag i Sverige.[7]

5.2. Metod Nulägesanalys

Nedan redogörs för hur nulägesanalysen har utförts. Arbetsmoment som beskrivs är segmentering, sammanslagning av data, framtagning av indexmatriser och analys genom analyskors.

Segmenteringar i förstudien har utgått från segmenteringar i sekundärdata. För målgruppen allmänheten har de demografiska segmenten *kön, ålder, utbildning och inkomst* använts. Sekundärdata innehåller något olika åldersintervall och för att göra det hanterbart i förstudien har några åldersintervaller integrerats till större intervaller. De slutliga segmenten i förstudien utgörs av fem åldersintervaller: 16–25, 26–45, 46–64, 65–74 och 75+ år. För målgruppen mindre företag används firmografiska segmentet *företagsstorlek* samt teknografiska segmenten *bransch, sektor* och *digital mognad*[8]. Sekundärdata använder lite olika intervaller gällande företagsstorlek. För att göra det hanterbart i förstudien har integreringen gjorts till totalt tre storlekssegment: 0–9, 10–99 och 100–249 anställda.

Ingen enskild undersökning täcker alla områden som ska besvaras i förstudien (de fyra frågeställningarna i kap 3.1) och därför slås flera undersökningar samman till index som breddar kartläggningen om målgrupperna. Relevanta enkätfrågor inom samma ämnesområde väljs ut från sekundärdata och bildar index. Urvalet har även gjorts med stöd av dokumentationen Grundläggande cybersäkerhet, bilaga 1. Sekundärdata, som består av 70 frågor ställda till företag och 80 frågor till allmänheten, har sorterats in under följande index:

Orosindex, här graderar respondenterna sin oro för risken att drabbas av digitala attacker, brott och bedrägerier. Indexet ger indikation om hur ett segment ser på kriminella och antagonistiska hot och risker

7 https://tillvaxtverket.se/tillvaxtverket/statistikochanalys/statistikomforetag/foretagande/basfaktaomforetag.1719.html
8 https://www.telia.se/foretag/smart-arbetsliv-koncept/telias-digitala-index-2022

inom informations- och cybersäkerhetsområdet. Exempel på frågor i orosindex: *Hur orolig är du för att få din dator kapad/hackad genom skadlig kod/virus? Hur orolig är du för att ditt företag ska utsättas för digitala virusattacker?*

Robusthetsindex, här graderar respondenterna sin medvetenhet, kunskap och vidtagna säkerhetsåtgärder inom informations- och cybersäkerhetsområdet. I detta index framträder bilden av hur skyddade, eller oskyddade, allmänheten och mindre företag är i den digitala miljön. Exempel på frågor är: *Har du ditt kort spärrat för internetbetalning så att du behöver låsa upp det om du ska betala på nätet? Har lagring av viktig info och backup på icke internetuppkopplad plats vidtagits för att motverka it-brottslighet, ja/nej?*

Utsatthetsindex, här samlas bilden av respondenternas självskattade utsatthet för försök till bedrägerier eller annan it-brottslighet. Exempel på frågor i detta index är: *Har du blivit uppringd av någon som försökt lura dig att identifiera dig via BankID eller Bankdosa? Har ert företag varit utsatta för digitalt intrångsförsök under det senaste året?*

Brottsindex, här anger respondenterna i vilken grad de anser att de utsatts för fullbordade brott i digitala miljöer. Exempel på frågor: *Har du som företagare/ditt företag blivit utsatt för it-relaterade brott med bluffaktura under det senaste året, ja/nej? Har du blivit utsatt för någon typ av it-relaterad brottslighet? (brott där internet används för att utföra till exempel id-kapning, stjäla lösenord eller skicka ut falsk information i syfte att komma åt information), ja/nej?*

Motivationsindex, här indikeras hur intresserade respondenterna är av att lära sig mer för att öka det egna skyddet inom informations- och cybersäkerhet, och om de är intresserade av att dela information och hjälpa andra. Exempel på frågor i motivationsindex är: *Jag är i behov av hjälp och vägledning över hur jag ska skydda mig mot digitala bedrägerier, ja/nej? Jag delar ofta med mig av mina erfarenheter kring nätsäkerhet och digitala brott i syfte att skydda och informera andra, ja/nej?*

Inom varje index kan antalet enkätfrågor per segment variera något, vilket har tagits hänsyn till genom viktning för att resultaten ska bli jämförbara. Frågor i sekundärdata har olika svarsskalor, vilket också har tagits hänsyn till.

För målgruppen allmänheten har fem index skapats: orosindex, robushetsindex, utsatthetsindex, brottsindex och motivationsindex. För målgruppen mindre företag har fyra index skapats: orosindex, robusthetsindex, utsatthetsindex och brottsindex. Motivationsindex har inte skapats för företagsmålgruppen då det saknas data som beskriver företagens motivation.

5.2.1. Produktion av två indexmatriser

Data från respektive målgrupp sammanställs i indexmatriser, vilka ger en överskådlig bild över de olika segmentens resultat. Alla index har en skala mellan 0–100 % och visar graden av oro, robusthet och utsatthet som respondenterna har angett. Det går att utläsa hur enskilda segment står sig i förhållande till Grundläggande cybersäkerhet enligt bilaga 1, och det går att jämföra hur segment förhåller sig till varandra.

5.2.2. Analys av segmentens nuläge

Analys av segment och indexvariabler görs i så kallade analyskors. Segmentens placeras ut i analyskorsens fyrfältare och analyseras via två index åt gången. Metoden underlättar granskningen av segmentens egna

positioner samt mellan varandra, och beskriver segmentens nulägen i förhållande till Grundläggande cybersäkerhet enligt bilaga 1.

5.2.3. Behovsanalys

I sista steget görs en sammanvägning av målgruppens nuläge i relation till Grundläggande cybersäkerhet enligt bilaga 1. Resultatet ger en bild av vilka behov som finns hos målgrupperna och segmenten att öka den egna informations- och cybersäkerheten, samt en bild över hur målgrupperna ser på den egna oron och utsattheten inom området vilket bidrar till att besvara hur målgrupperna kan prioriteras.

6. Resultat och analys företag

I följande kapitel redovisas resultatet över segmentens positioner i förstudiens index och därefter presenteras behovsanalysen.

6.1. Resultat företag

I indexmatrisen över företag i figur 1, ges en samlad presentation över respektive segments värde inom orosindex, robusthetsindex, utsatthetsindex och brottsindex.

Företag Indexmatris	Orosindex	Robusthetsindex	Utsatthetsindex	Brottsindex
Firmografiska segment				
0-9 anställda	29	37	17	26
10-99 anställda	40	51	23	28
100-249 anställda	46	64	24	14
Teknografiska segment				
Högdigital verksamhet	65	-	35	-
Medeldigital verksamhet	49	-	24	-
Lågdigital verksamhet	24	-	15	-
Tillverknings-, utvinningsindustri	45	33	18	25
Byggindustri	26	32	11	22
Hsndel, transport, hotell, restaurang	27	29	17	21
Informations- och kommunikationsföretag	22	45	9	19
Företagstjänster	37	40	17	24
Vård, omsorg, utbildning och tjänster	30	31	18	22
Industri, jordbruk, skog, fiske, bygg	32	33	14	23
Tjänster	31	35	17	22

Figur 1. Indexmatris Företag

I orosindex framkommer företagens gradering av upplevd oro för att drabbas av olika digitala brott och bedrägerier.

- I segmentet **företagsstorlek** anger de minsta företagen med 0–9 anställda lägst oro (29 %), medan företag med 10–99 anställda och företag med 100–249 anställda anger högre oro (40 % och 46 %).
- I segmentet **digitala verksamheter** anger högdigitala företag betydligt mer oro (65 %) än medeldigitala (49 %) och lågdigitala (24 %).
- Bland **branscher** är det tillverknings- och utvinningsföretag som anger högst oro (45 %) och följs av företagstjänster (37 %). Lägst oro anger informations- och kommunikationsföretag (22 %).
- Inom **sektorerna** industri och tjänster är nivån på orosindex likvärdig (32 % och 31 %).

Robusthetsindex beskriver graden av företagens medvetenhet, kunskap och vidtagna säkerhetsåtgärder inom informations- och cybersäkerhetsområdet.

- Ju mindre **företagsstorlek**, desto lägre robusthet. Företag med 0–9 anställda (37 %), 10–99 anställda (51 %) och 100–249 anställda (64 %).
- Inom **branscher** anger informations- och kommunikationsföretag högst robusthet (45 %), tätt följt av företagstjänster (30 %). Lägst robusthet uppger handel, transport, hotell och restaurang (29 %).
- Resultatet i **sektorerna** industri och tjänster visar på likvärdig robusthet (33 % och 35 %).

Utsatthetsindex ger en bild av företagens självskattade utsatthet för bedrägeri- och brottsförsök.

- I **storlekssegmentet** anger företag med 10–99 anställda (23 %) samt 100–249 anställda (24 %) en likvärdig utsatthet för bedrägeriförsök. Företagen med 0–9 anställda anger en lägre utsatthet (17 %).
- Företag med **högdigital verksamhet** anger högre utsatthet för bedrägerier (35 %) än medeldigitala (24 %) och lågdigitala (15 %).
- Inom **branscher** anger tillverknings- och utvinningsindustri samt vård, omsorg, utbildning och tjänster högst utsatthet (båda 18 %). Byggindustrin (11 %) och informations- och kommunikationsföretag (9 %) är branscher som anger lägst utsatthet.
- I **sektorssegmentet** anger företag inom tjänstesektorn något högre utsatthet för bedrägerier (17 %) än industrisektorn (14 %).

I Brottsindex framkommer i vilken grad företag själva anger att de drabbats av fullbordade brott.

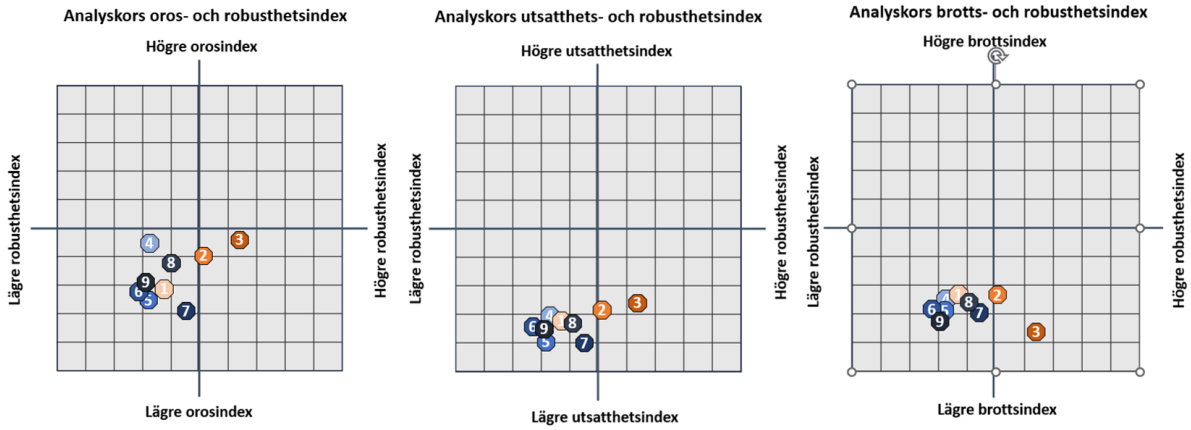
- I segmenten **företagsstorlek** anger företag med 0–9 anställda (26 %) och företag med 10–99 anställda (28 %) högre utsatthet för brott med konsekvens än företag med 100–249 anställda (14 %). Vid ett nedbrutet resultat framgår det att i företag med storleksintervall 0–9 anställda anger stora skillnader inom gruppen. Företag med 5–9 anställda anger störst konsekvens vid brott (34 %) jämfört med de minsta företagen med 0–4 anställda som anger lägst konsekvens vid brott (18 %).
- Inom **branschsegment** har informations- och kommunikationsföretag lägst brottsindex (19 %) och tillverknings- och utvinningsföretag högst (25 %).
- Resultat för brottsutsatthet i **sektorer** är samstämmigt för industrin (23 %) och tjänster (22 %).

6.2. Analys av företagens nuläge

Nulägesanalysen görs via tre analyskors som illustreras i analyskorsen 1, 2 och 3. I varje analyskors samkörs två olika index där segmentens unika positioner illustreras. Diagrammen ska studeras som fyrfältare med fyra olika scenarion. Exempelvis i analyskors 1 visas segmentens grad av robusthet och grad av oro. Utifrån dessa kors gör analyser som beskrivs i följande avsnitt.

Notera att analyskorsen ska studeras som en fyrfältare med fyra olika scenarion, och inte som ett diagram med strävan åt övre högra hörnet.

Analyskors utifrån segmenten företagsstorlek och bransch



Analyskors 1.
Oros- och robusthetsindex

Analyskors 2.
Utsatthets- och robusthetsindex

Analyskors 3.
Brotts- och robusthetsindex

Segment företagsstorlek

1. Företag 0–9 anställda
2. Företag 10–99 anställda
3. Företag 100–249 anställda

Segment bransch

4. Tillverknings- & Utvinningsindustri, inkl. Energi & Miljö
5. Byggindustrin
6. Handel, Transport & Magasinering, Hotell, Restaurang
7. Informations- och Kommunikationsföretag
8. Företagstjänster
9. Vård & Omsorg, Utbildning, Tjänster, Personliga & Kulturella tjänster

Analyskors 1 (oro och robusthet) visar att företag med 10–99 och 100–249 anställda anger både hög robusthet och hög oro. Positionen kan förklaras med att större företag troligen har möjlighet att avsätta mer resurser för sin informations- och cybersäkerhet, och därigenom får ökad kunskap och förståelse för de höga nivåerna av hot och risker som drabbar svenskt näringsliv. Ytterligare en förklaring kan hämtas från mediebilden som slår upp stora rubriker om att stora företag riskerar att drabbas och drabbas alltmer av cyberattacker, vilket kan leda till större medvetenhet och oro hos företag som är lite större.

Mikroföretag anger i stället både lägre robusthet och lägre oro. En förklaring kan vara att man är mindre medveten om riskerna, eller att man anser att man har vidtagit tillräckligt med skydd. Kartläggningen visar att de minsta företagen med 0–9 anställda anger en robusthet omkring 37 % vilket är ett stort gap till 100 % robusthet som speglar nivån för Grundläggande cybersäkerhet enligt bilaga 1. Tillverkningsindustrin är det branschsegment som urskiljer sig mest med en förhållandevis hög oro och låg robusthet. Det är osäkert att dra slutsatser kring denna branschs låga robusthet, även om en tolkning kan vara att man påverkas eller stressas av regelverk eller mediabilder. Det finns behov av att ta reda på mer i ett nästa steg.

Analyskors 2 (robusthet och utsatthet) beskriver segmentens position och nuläge när det gäller utsatthet för brotts- och bedrägeriförsök (digitala) samt robusthet. Alla branschsegment är relativt samlade kring ett utsatthetsindex på 10–20 % och en robusthet om 30–40 %. Det skulle kunna förstås som att samtliga branscher upplever en motsvarande grad av utsatthet, oberoende av om segmentet har angivit en svagare eller starkare robusthet. Inom segmentet företagsstorlek finns ett liknande mönster där alla företag i kartläggningen anger en utsatthet på ca 20–25 %. Detta relativt sett oberoende av företagens storlek eller

robusthet. Detta säger något om att brotts- och bedrägeriförsök tycks utföras brett mot företag oavsett bransch eller storlek. Men vad var det som gjorde att man upptäckte försöket och avvärjde det? Frågor som kan vara värdefulla att undersöka vidare för att komma närmare svaret. Varför företag i storleken 100–249 anställda sticker ut kan ha att göra med att de har bättre förståelse och är bättre på att upptäcka brotts- och bedrägeriförsöken. Detta kan bero på deras ökade kunskap och medvetenhet, men även att de har råd att investera i åtgärder och teknologier som kan upptäcka försök. Deras något högre utsatthet kan bero på att det potentiellt finns mer pengar för de kriminella att hämta.

I **analyskors 3 (robusthet och brott)** framträder segmentens positioner i relation till robusthetsindex och brottsutsatthet. Mönstret är snarlikt det för analyskors 2, men med avvikelsen att företag med 100–249 anställda anger högst robusthet och lägst brottsutsatthet. En tolkning kan vara att segmentets högre robusthet skyddar mer än hos de mindre företagen med lägre robusthetsindex. Ett annat perspektiv kan vara att respondenter i mindre företag känner till alla brott och därför kan ange en brottsutsatthet närmare faktiska nivåer än större företag där många arbetar och respondenterna inte har samma överblick.

6.3. Behovsanalys och diskussion

Målet med förstudien är att segmentera och identifiera vilka behov målgrupperna har för att öka den egna informations- och cybersäkerheten samt ge förslag på vilka segmentet som ska prioriteras. Resultaten visar att det finns stora behov hos både mikroföretag med 0–9 anställda samt företag med 10–99 anställda att vidta fler säkerhetsåtgärder för att uppnå Grundläggande cybersäkerhet, bilaga 1.

Kartläggningen visar att utifrån ett nationellt företagsperspektiv tycks företag med upp till 99 anställda ha en mer sårbar situation än större företag. Dels utifrån brist på egna resurser, dels beroende på att stora delar av statens stöd för systematisk informations- och cybersäkerhet främst riktas mot myndigheter, organisationer och större företag.

Företagens bristande säkerhetsåtgärder exemplifieras genom utdrag från data i indexen.

a) 56 % bland företag med 0–4 anställda anger att deras företag inte alls, i liten utsträckning, eller varken eller, har förberett sig för digitala hot. (Telenor 2023).
b) 62 % bland företag med 0–9 anställda anger att de inte använder två- eller flerfaktorsautentisering vid inloggning som en åtgärd för att motverka it-brottslighet. (Företagarna 2022).
c) Vart fjärde företag (25 %) med 5–19 och 10–99 anställda anger att de utsatts för bedrägeriförsök med små eller stora konsekvenser under den senaste 12-månadersperioden. Att jämföra med 0–4 anställda (8 %) och 100–249 (15 %). (Telenor 2023).

Det bör tilläggas att det kan finnas fler och andra förklaringar till segmentens nulägen. Men det saknas relevant data som hjälper till att fördjupa svaren, exempelvis kring företagens utsatthet. Den officiella kriminalstatistiken visar inte hur stor andel anmälda brott som kommer från företag. Därtill finns det ett stort mörkertal i denna slags statistik då långt ifrån alla brott och bedrägerier inte polisanmäls.

Företagens behovsanalys kan sammanfattas genom två fynd som framkommit i förstudien. Högre kunskap och ökad medvetenhet om hot och risker i digitala miljöer gör sannolikt att företag blir mer medvetna om risker och bättre på att upptäcka brottsförsök och riktade attacker, samtidigt som det kan orsaka ökad oro. Segment som befinner sig i denna mognadsgrad kan antas vara motiverade att ta till sig och implementera mer hjälp och stöd särskilt anpassade för dem. Ett annat fynd är att lägre kunskap om digitala hot och risker

skulle kunna försätta segmenten i en falsk trygghet med lägre grad av vidtagna åtgärder och lägre oro. Dessa segment kan behöva stora stödpaket med mycket kunskap för att öka medvetenheten om riskerna, öka kunskapen om vad och hur man skyddar sig.

7. Resultat och analys allmänheten

I följande kapitel redovisas resultatet över segmentens positioner i förstudiens index och därefter presenteras behovsanalysen.

7.1. Resultat allmänheten

I indexmatrisen över allmänheten i figur 2, ges en samlad presentation över respektive segments värde inom orosindex, robusthetsindex, utsatthetsindex, brottsindex och motivationsindex.

Allmänhet Indexmatris	Orosindex	Robusthetsindex	Utsatthetsindex	Brottsindex	Motivationsindex
Demografiska segment					
Män	32	52	28	13	35
Kvinnor	38	47	25	12	33
16-25 år	41	49	36	15	36
26-45 år	43	56	45	13	36
46-64 år	41	57	41	9	33
65-74 år	34	51	25	10	34
75+ år	26	34	17	-	32
Inkomst hög	41	68	45	19	-
Inkomst mellan	36	59	39	7	-
Inkomst låg	41	54	35	7	-
Högskola Universitet	35	59	42	12	-
Gymnasium	38	54	36	11	-
Grundskola	37	53	32	13	-
Anställd heltid	39	57	33	9	-
Egen företagare	24	68	28	13	-

Figur 2. Indexmatris Allmänhet

Orosindex ger en samlad bild över segmentens upplevda oro över att drabbas av bedrägerier och brott i digitala vardagsmiljöer.

- I segmentet **kön** anger män lägre oro (32 %) än kvinnor (38 %).
- Lägst oro bland **ålderssegmenten** anges av allra äldsta 75+ år (26 %) direkt följt av 65–74 år (32 %). Övriga segmentet anger något högre oro som 16–25 år (38 %), 26–45 år (41 %) och 46–64 år (39 %).
- Inom segmentet **inkomstnivå** är graden av oro relativt samstämmig mellan höginkomsttagare (41 %), mellan- (36 %) och låginkomsttagare (41 %).
- **Utbildningsnivå** tycks inte ha någon större inverkan på graden av oro. Resultaten är ganska samstämmiga mellan högskola/universitet (35 %), gymnasium (38 %) och grundskola (37 %).

- För segmentet **sysselsättning** är anställda betydligt mer oroliga (39 %) än egenföretagare (24 %).

Robusthetsindex beskriver i vilken grad allmänheten självskattat sin medvetenhet, kunskap och vidtagna säkerhetsåtgärder inom informations- och cybersäkerhetsområdet.

- I segmentet **kön** anger män något högre robusthet (52 %) än kvinnor (47 %).
- I **ålderssegmentet** är det den allra äldsta gruppen 75+ år (34 %) som anger lägst robusthet. Högst robusthet anges i intervallet 46–64 år (57 %) och 26–45 % (56 %).
- Inom **inkomstnivå** anges högre robusthet ju högre inkomsten är. Höginkomsttagares robusthet är högst (68 %) och därefter följer mellaninkomsttagare (59 %) och låginkomsttagare (54 %).
- Inom **utbildning** finns en liten variation i robusthet mellan segmenten universitet/högskola (59 %), gymnasium (54 %) och grundskola (53 %).
- I segmentet **sysselsättning** finns en synbar skillnad mellan egenföretagare som anger högre robusthet (68 %) än anställda (57 %).

Utsatthetsindex beskriver i vilken grad allmänheten anger att de utsatts för försök till bedrägeri eller brott.

- **Kvinnor och män** anger liknande nivåer av utsatthet för bedrägeriförsök (kvinnor 25 % och män 28 %).
- Inom **ålderssegmentet** anger de äldre lägre utsatthet för bedrägeriförsök än övriga åldersintervaller. Utsatthetsindex är lägst i åldersgruppen 75+ år (17 %) och näst lägst för gruppen 65–74 år (25 %). Högst utsatthet anger grupperna 26–45 år (45 %) och 46–64 år (41 %).
- Resultat i **inkomstsegmentet** indikerar att utsattheten faller med minskade inkomster. Högst utsatthet anger höginkomsttagare (45 %) jämfört med mellaninkomsttagare (39 %) och låginkomsttagare (35 %).
- I **utbildningssegmentet** tycks trenden vara att ju lägre utbildningsnivå desto lägre är utsatthetsindex. Respondenter med universitet/högskoleutbildning anger högst utsatthet (42 %), gymnasieutbildade något lägre (36 %) och grundskoleutbildade lägst (32 %).
- Resultatet för utsatthetsindex i segmentet **sysselsättning** visar att egenföretagare anger något lägre utsatthet (28 %) än anställda (33 %).

Brottsindex visar i vilken grad allmänheten själva anger att de drabbats av brott.

- **Kvinnor och män** anger motsvarande nivå på brottsutsatthet (kvinnor 12 % och män 13 %).
- Resultaten i **ålderssegmenten** visar att yngre respondenter anger något högre brottsutsatthet än övriga. Åldersintervallet 16–25 år (15 %), 26–45 år (13 %), 46–64 år (9 %) och 65–74 år (10 %).
- I **inkomstsegmentet** framkommer betydande skillnader i självskattad brottsutsatthet mellan höginkomsttagare (19 %) jämfört med mellaninkomsttagare (7 %) och låginkomsttagare (7 %).
- **Utbildningsnivå** tycks inte ha någon större påverkan på graden av brottsutsatthet. Resultaten är relativt jämförbara mellan segment med utbildning på högskola/universitet (12 %), gymnasium (11 %) och grundskola (13 %).
- Inom **sysselsättning** anger egenföretagare att de är mer brottsutsatta (13 %) än anställda (9 %),

Motivationsindex anger i vilken grad allmänheten anger att de är intresserade av att lära sig mer samt hjälpa andra för att öka det egna skyddet inom informations- och cybersäkerhet.

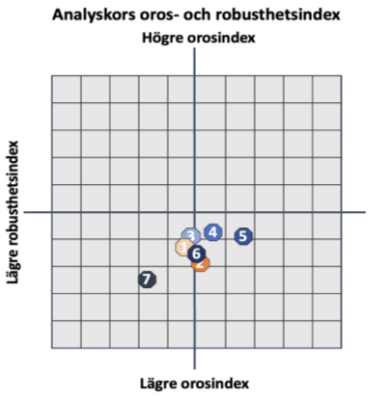
- Resultatet för **mäns och kvinnors** motivationsindex visar på relativ samstämmighet. Män (35 %) och kvinnor (33 %).
- Inom **ålderssegmentet** framkommer ett relativt samlat resultat, men med något högre motivation hos 16–25 år (36 %) och 26–45 år (36 %).

7.2. Analys av allmänhetens nuläge

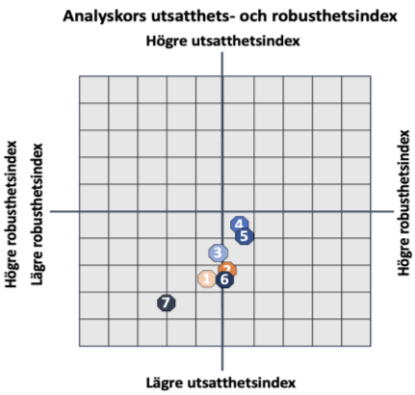
Här presenteras behovsanalysen som bygger på resultat från indexmatrisen. Nulägesanalysen görs via sex analyskors som presenteras i analyskors 4, 5, 6, 7, 8 och 9 nedan. I varje analyskors har segmenten fått sin unika position baserat på deras resultat från indexmatrisen.

Notera att analyskorsen ska studeras som en fyrfältare med fyra olika scenarion, och inte som ett diagram med strävan åt övre högra hörnet.

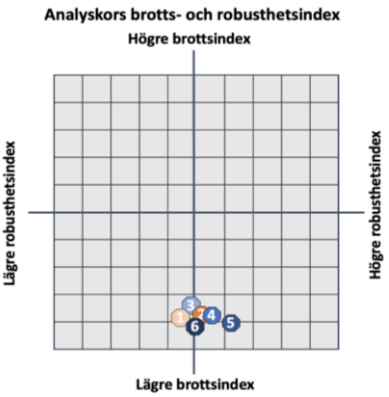
Analyskors utifrån segmenten kön och ålder



Analyskors 4.
Oros- och robusthetsindex



Analyskors 5.
Utsatthets- och robusthetsindex



Analyskors 6.
Brotts- och robusthetsindex.

Segment kön	**Segment ålder**
1. Kvinnor	3. 16–25 år
2. Män	4. 26–45 år
	5. 46–64 år
	6. 65–74 år
	7. 75+ år

Analyskors 4 (oro och robusthet / kön och ålder) anger att de allra äldsta 75+ år är minst oroliga i ålderssegmenten. De är även minst robusta. I tidigare analyser visar sig även detta mönster men inte specifikt för denna åldersgrupp, utan att den som är minst digital mogen är också den som har lägst oro, vilket tros bero på okunskap[9]. Redan i nästa åldersgrupp 65–74 år är både oron högre liksom robustheten. Det kan betyda att i en mer digital vardag ökar insikter om vilka hot och sårbarheter som finns, vilket i sig leder till en strävan efter ökad robusthet. De flesta segmentens positioner ligger relativt samlade kring 40 % oro och 50–60 % robusthet. Segmentet 46–64 år urskiljer sig något genom att ange högst oro och hög robusthet. En tänkbar tolkning av den höga oron är att individer i denna åldersgrupp befinner sig mitt i livet och får ta del av många olika riskmiljöer samtidigt, som exempelvis via arbetsplatsen, det egna privatlivet men också genom

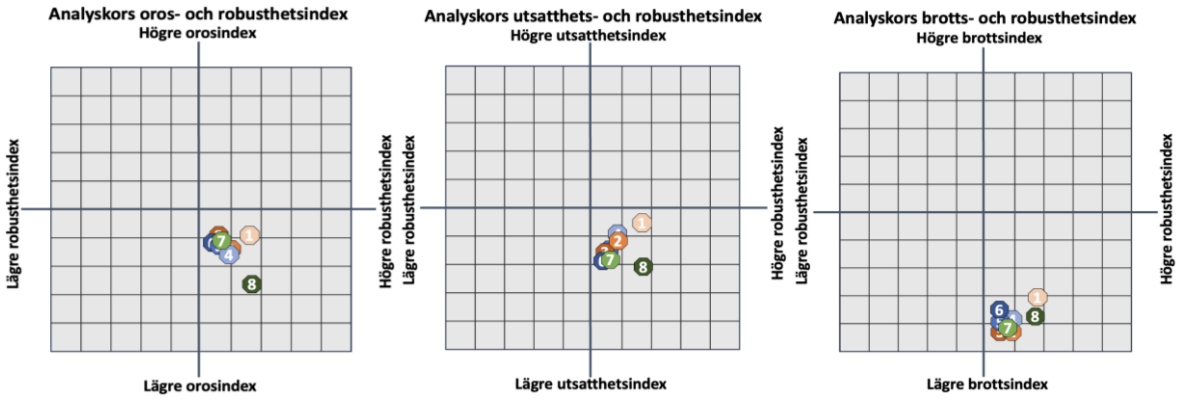
9 Målgruppsanalys digitala bedrägerier. 2020. Nepa/SSF

barn och äldre föräldrar som man inte sällan har en central roll för. De kan även antas vara i en köpkraftig ålder som gör att de kan köpa åtgärder som ger en högre robusthet. Varför män har högre robusthet men lägre oro än kvinnor, kan ha sin förklaring i att män kanske traditionellt är mer teknikintresserade, köpkraftiga och självsäkra. Tidigare analyser styrker detta och vittnar om att den som är mest digitalt mogen även är den med högst robusthet[10].

Analyskors 5 (utsatthet och robusthet / kön och ålder) visar hur ålderssegment som anger hög robusthet också anger högre utsatthet för bedrägeriförsök. Beror detta på att de som befinner sig i en digital miljö är mer sårbara, som segmenten 26–45 år och 46–64 år? Att om man befinner sig i arbetslivet eller inte, kan potentiellt påverka både ens robusthet och ens utsatthet. Är man mitt i arbetslivet kanske man har ett större digitalt inflöde som ger högre utsatthet, samtidigt som man förmodligen är mer medveten och köpkraftig, vilket kan driva robusthet. Medan de som inte befinner sig mitt i arbetslivet kanske har lägre digitalt inflöde med lägre utsatthet, samtidigt som kunskap och medvetenhet kan vara lägre. Kanske är det så att sårbarhet driver robusthet. En annan tolkning kan vara att 26–45 och 46–64 åringar har mer kunskap om hur man upptäcker bedrägerier, och därför anger högre utsatthet än andra åldersgrupper.

Analyskors 6 (brott och robusthet / kön och ålder) visar hur samtliga segment anger motsvarande nivå på brottsutsatthet. Till skillnad mot analyskors 5 med utsatthet för bedrägerier tycks inte brottsutsattheten skilja sig på samma vis mellan ålderssegmenten. Segmenten 26–45 år och 46–64 år med högst robusthet, positionerar sig på samma nivå för brottutsatthet som övriga segment. En tolkning kan vara att utsattheten för brott inte hänger ihop med den egna robustheten. Men det går också att se utifrån ett annat perspektiv, att vissa brott inte upptäckts som exempelvis stöld av information eller placering av skadlig kod i digitala enheter. Det kanske också är så att robustheten avvärjer brotten, och händelsen i stället anges som utsatthet för försök till brott eller bedrägerier. Det kan även finnas ett stort mörkertal bland brotten, då människor inte vill berätta om de brott de utsatts för och eftersom underlaget till detta bygger på självskattning, så skulle det kunna se annorlunda ut om alla anmälde de brott som det utsätts för. Åldersgruppen 75 + saknas i detta analyskors då materialet till kartläggningen saknar information om gruppens brottsutsatthet.

Analyskors utifrån segmenten inkomst, utbildning och sysselsättning



Analyskors 7.
Oros- och robusthetsindex

Analyskors 8.
Utsatthets- och robusthetsindex

Analyskors 9.
Brotts- och robusthetsindex.

10 Målgruppsanalys digitala bedrägerier. 2020. Nepa/SSF

Segment inkomst	Segment utbildning	Segment sysselsättning
1. Hög	4. Högskola	7. Anställda
2. Mellan	5. Gymnasium	8. Egenföretagare
3. Låg	6. Grundskola	

Analyskors 7 (orosindex och robusthetsindex / inkomst, utbildning och sysselsättning) visar hur samtliga segmenten ligger samlade omkring 40 % oro och 60 % robusthet. Det är i segmentet sysselsättning som egenföretagare skiljer ut sig med 24 % oro och 68 % robusthet. En position som anger betydligt lägre oro och högre robusthet än anställda. En tolkning är att egna företagare befinner sig i en digital arbetsmiljö som man själv har kontroll över och kan påverka. Det innebär att man som egenföretagare i högre grad än anställda kan bestämma och vidta de säkerhetsåtgärder som man själv önskar. Känslan av kontroll över de egna säkerhetsåtgärderna kan i sin tur leda till minskad oro. Anställda kanske är oroliga på grund av att de inte vill göra fel inför arbetsgivaren eller att de inte kan lita på arbetsgivarens säkerhet. Varför höginkomsttagare är mer robusta och oroliga än övriga kan bero på deras högre inkomst, medvetenhet och köpkraft som leder till ökad oro. Denna teori stämmer överens med vad tidigare analyser vittnar om, den som ligger digitalt i framkant är också den som är mest orolig[11].

Analyskors 8 (utsatthetsindex och robusthetsindex / segment inkomst, utbildning och sysselsättning) visar hur segmenten inkomst och utbildning positionerar sig kring utsatthetsindex och robusthetsindex. Resultaten visar att segment med högre robusthet också drabbas något mer av bedrägeriförsök och försök till annan it-brottslighet. En förklaring till varför segment med högre utbildning och högre inkomst drabbas i högre utsträckning, kan vara att deras vardag innehåller fler risker. Kanske är de mer våghalsiga i sina digitala beteenden, kanske har de fler digitala prylar och enheter som är uppkopplade, och kanske innehåller deras vardag mer tid i digitala miljöer än övriga segment.

Analyskors 9 (brottsindex och robusthetsindex / segment inkomst, utbildning och sysselsättning) illustrerar inkomst- och utbildningssegmentens position kring brottsutsatthet och robusthet. Högutbildade placerar sig högre i brottsutsatthet på motsvarande vis som de gör i utsatthet för bedrägeriförsök och försök till annan it-brottslighet i analyskors 5. Det finns behov av att undersöka mer vad som verkligen ligger bakom höginkomsttagarens utsatthet, men ett sätt att tolka det på är att höginkomsttagaren har medel att skaffa sig mer digitala prylar som ökar attackytorna, och kanske kan detta segment kosta på sig att vara mer riskbenägna genom en tryggare ekonomisk situation. Det kan även vara så att de är utvalda av kriminella för att de har hög inkomst. Det finns behov av att ta reda på mer i nästa steg. Samtidigt visar även analyskorset att utbildningsnivå kanske inte spelar någon roll för hur utsatt man är för brott eller hur duktig man är på säkerhetsåtgärder för att öka sin robusthet.

7.3. Behovsanalys och diskussion

Målet med förstudien är att segmentera och identifiera vilka behov målgruppen allmänheten har av stöd för att öka den egna informations- och cybersäkerheten. Resultaten visar att allmänheten har behov av ökad robusthet för att uppnå Grundläggande cybersäkerhet enligt bilaga 1.

11 Målgruppsanalys digitala bedrägerier. 2020. Nepa/SSF

Kartläggningen tyder på att samtliga segment inom allmänheten har vidtagit för liten andel egna säkerhetsåtgärder och att de därmed är onödigt sårbara, vilket leder till större risker för att drabbas av cyberattacker. Den låga nivån på robusthet kan bero på bristande kunskap, men också på digital ovana, stresskänslighet och brist på kritiskt förhållningssätt och andra egenskaper hos individer.[12]

Allmänhetens bristfälliga ageranden exemplifieras genom utdrag från data i robusthetsindex.

a) 80 % i segmentet kvinnor anger att de inte har sitt kort spärrat för internetbetalning, på ett sätt så att de måste låsa upp det om de ska betala på nätet. Motsvarande svar bland män är 74 %. (Demoskop 2023)
b) 68 % av männen och 72 % av kvinnorna anger att de aldrig använt tekniker som kodord, motringning, rörelsemönster eller annat, för att vara säker på att den de pratar med på dator/telefon inte är en bedragare. (Demoskop 2023)
c) 60 % i segmenten 18–29 år samt 30–49 år reflekterar sällan över om appar kan påverka säkerheten, urval instämmer, instämmer helt eller varken eller. (Tänk Säkert 2023)

Allmänhetens behovsanalys kan sammanfattas genom två fynd som framkommit i förstudien. Mer erfarenheter och kunskap om digitala miljöer ser ut att innebära en ökad medvetenhet om hot och risker, vilket kan förklara den höga oron hos robusta individer. Dessa segment är sannolikt mer motiverade att ta till sig ny kunskap anpassade för dem, och som de direkt kan implementera i sin digitala vardag. Ett annat fynd är att lägre kunskap om digitala hot och risker kan försätta segmenten i en falsk trygghet med lägre oro och lägre grad av vidtagna åtgärder. Segment i denna position kan behöva stora stödpaket med mycket kunskap för att öka medvetenheten om riskerna, öka kunskapen om vad och hur man skyddar sig.

8. Prioritering av segment

Segmenteringen av målgrupperna i det framtida arbetet via en nationell samlingsplats bör göras utifrån den aktuella önskade målbilden inom informations- och cybersäkerhet.

- Om målet är att höja lägstanivån på allmänhetens egna vidtagna säkerhetsåtgärder bör segment med lägst robusthetsindex prioriteras. Vid en sådan målbild bör segment ur allmänheten prioriteras utifrån lägre utbildning, lägre inkomst, samt de yngsta och äldsta ålderssegmenten. Motsvarande insats bland företag bör inriktas mot företag med 0–99 anställda samt branscher som handel, transport, hotell, restaurang samt vård, omsorg och utbildning, som alla anger lägre robusthet än övriga segment.
- Är målet att minska brottsutsattheten kan de segment som anger högst brottsindex prioriteras. I målgruppen allmänhet utmärker sig segmenten höginkomsttagare, män och 16–26 åringar. Inom målgruppen företag är det mindre företag med mellan 0–99 anställda samt tillverknings- och utvinningsindustrin som skulle kunna prioriteras.
- Är målet att skapa ett ökat engagemang kring information- och cybersäkerhet bland allmänheten föreslås att segment med nyfikenhet och intresse av att lära mer prioriteras. Motivationsindex visar ett ganska samlat resultat bland segmenten i allmänheten, men högst motivation anger de yngre ålderssegmenten 16–25 år och 26–45 år.

12 https://bra.se/publikationer/arkiv/publikationer/2023-09-12-bedragerier-mot-privatpersoner.html

Förstudien föreslår att företag med 0–99 anställda prioriteras i det fortsatta arbetet med att öka den grundläggande informations- och cybersäkerheten via en nationell samlingsplats. Kartläggning visar att det inte bara är mikroföretag (0–9 anställda) som anger låg robusthet, utan att det även gäller företag med 10–99 anställda. Företag med 10–99 anställda ser ut att hamna i en klämd situation med en robusthet *under* företagen med 100–249 anställda, men med en brottsutsatthet *långt över* de större företagen med 100–249 anställda. Företagen med 10–99 anställda har troligen inte motsvarande egna resurser, förmåga, kompetens eller organisering att ta till sig det statliga systematiska stöd för informations- och cybersäkerhet som större företag kan antas ha tillgång till.

9. Summering och nästa steg

9.1. Summering

Förstudien ger övergripande svar på olika målgrupper och segments behov av informations- och cybersäkerhet. Företagens kartlagda nuläge och behov visar att mindre företag vidtar färre säkerhetsåtgärder jämfört med medelstora och stora företag, vilket ligger i linje med förstudiens hypotes. Även resultat från kartläggning av allmänheten, som visar att alla segment behöver vidta fler säkerhetsåtgärder för att förbättra informationshantering, informationssäkerhet och cybersäkerhet, stödjer förstudiens hypotes.

Kartläggningen ger en tydlig fingervisning om hur de olika ålders-, utbildnings- och inkomstsegmenten positionerar sig i förhållande till varandra. Och beroende på vad man vill åstadkomma för resultat genom ökade insatser för höjd informations- och cybersäkerhet, kan man välja att fokusera på olika grupper. Segment som uppger lägre informations- och cybersäkerhet än andra är kvinnor, unga och äldre, och kan prioriteras om målet är att höja lägsta nivån av robusthet i landet. Tillverknings- och utvinningsföretag sticker ut från övriga branscher genom att de anger både hög oro och hög utsatthet, samtidigt som de inte är särskilt robusta. Ett segment som kan prioriteras om målet är att höja säkerheten bland utsatta företag med lågt eget skydd.

En intressant insikt i förstudien är att låg oro skulle kunna tolkas som att man har goda kunskaper om risker i den digitala miljön och att man har vidtagit generöst med säkerhetsåtgärder, att man känner sig säker och inte orolig. Låg oro skulle också kunna tolkas som att man har låg kunskap och medvetenhet om risker i digitala miljöer och att man saknar insikt om vad man ska skydda sig mot, man upplever en falsk trygghet. Denna insikt skulle kunna tyda på ett behov av mer information och kommunikation med målgrupperna.

Kartläggningen tyder på att utbudet av befintligt stöd och hjälp inte är tillräckligt eller inte når målgrupperna i tillfredställande hög grad. Ökade insatser som utveckling av befintliga och nya stöd samt tillgängliggörande av dessa, kommer kunna bidra till höjd medvetenhet om risker och ökad kunskap om säkerhetsåtgärder hos fler individer och mindre företag, vilket i sin tur kan bidra till en ökad informations- och cybersäkerhet i hela landet.

I framtida studier skulle det vara intressant att titta på flera aspekter utifrån det resultat som förstudien ger. Det skulle behövas en nationell studie som ger mer detaljerade och djuplodande svar avseende målgruppernas behov, för att kunna dra mer säkra slutsatser kring hur man bäst kommunicerar med målgrupperna.

9.2. Rekommendationer för nästa steg

För att kunna stötta allmänheten och mindre företag i den grundläggande cybersäkerheten rekommenderas ökade stödinsatser. Allmänheten och mindre företag har behov av att stärka sina egna skydd och för det behövs utbildning, verktyg och upprepad träning. En grundläggande förutsättning för att engagera målgrupper att vidta de säkerhetsåtgärder och förändrade beteenden som krävs, är kontinuerlig dialog och kommunikation. Först då höjs hela Sveriges säkerhet och trygghet.

Människor oroar sig över hot och risker i digitala vardags- och arbetsmiljöer och det kan upplevas som svårt att hantera all teknik. Därför är behoven av lättillgänglig och samlad information, kunskap och stöd för hur individer och mindre företag ska skydda sig själva mot digitala bedrägerier och brott stort. Oavsett om hotet kommer från cyberkriminella, hacktivister, statsaktörer eller statsunderstödda grupper riskerar individer och företag att drabbas av egna skador eller utnyttjas för att orsaka skador på vårt samhälle.

En internationell utblick visar hur andra länder tagit sig an motsvarande utmaningar med att höja informations- och cybersäkerheten bland befolkning och företag. I exempelvis Nederländerna verkar Fraud Helpdesk med att förhindra att den holländska befolkningen blir offer för bedrägerier.[13] Fraud Helpdesk förebygger utsatthet genom att göra medborgare och företag medvetna om bedrägeririsker och ger praktiska tips om hur de kan begränsa dessa risker. Verksamheten subventioneras av staten.

I Storbritannien har en bedrägeristrategi etablerats av staten som erbjuder allmänheten kunskap, stöd och medvetenhet för att stärka befolkningen.[14] Här står bedrägerier för 40% av alla brott. Ett av strategins huvudsakliga insatsområden är att stötta medborgarna genom att ge dem verktyg och kunskap som hjälper dem att hålla sig säkra.

Australien etablerade ett nationellt anti-bedrägericenter sommaren 2023 med målsättningen att stötta allmänheten och försvåra för bedragare.[15] Centret är ett samarbete mellan myndigheter och privat sektor och insatsområdena är att identifiera och varna medborgarna för pågående bedrägerier för att öka medvetenheten om risker och hot.

Även Sverige har behov av en nationell samlingsplats, som med hög trovärdighet kan fungera som den naturliga ”rådgivaren” för allmänhet och mindre företag i syfte att förebygga cyberhot och digitala brott. Det finns flera aktörer som har delar av de verktyg och förmågor som bedöms behöver finnas i en nationell samlingsplats. Nu behövs det en samordning, uppgradering, anpassning och utveckling av befintligt och nytt utbud av stöd och hjälp. SSF har redan flera delar på plats genom säkerhetskollen.se. En förutsättning för en vidareutveckling till en nationell samlingsplats är bland annat resurser i form av monetära medel, samarbeten med andra organisationer avseende data och förstärkning av personella resurser.

Förstudien bidrar med ny kunskap om målgrupper och segment och är ett steg framåt mot en framtida nationell samlingsplats. Som ett nästa steg föreslås att några utvalda verktyg och moduler testas mot prioriterade segment för att se hur engagemang och vilja till förändrat beteende kan ökas. Vidare bör en nationell samlingsplats verka datadrivet för att hela tiden följa vad som engagerar segmenten och vad som får

[13] https://www.fraudehelpdesk.nl/

[14] https://assets.publishing.service.gov.uk/media/5a7b613bed915d429748eaca/national-fraud-strategy.pdf

[15] https://www.accc.gov.au/national-anti-scam-centre

människor att vidta åtgärder. Med dessa insikter kan utbudet av stöd och hjälp hela tiden anpassas så att det ger maximal effekt. Andra insatser som bör vidtas i ett nästa steg är exempelvis att skapa fler samverkansforum för branscher och mindre företag med fokus på informations- och cybersäkerhet.

Försvarsberedningen har, i sin rapport Kraftsamling från december 2023, pekat på att denna förstudie är ett steg mot en sammanhållen ingång, dit företag med begränsade it-säkerhetsresurser kan vända sig för att få stöd för ökad kunskap och kompetens inom informations- och cybersäkerhetsområdet

Stockholm 31/1 2024

Ulrika Hallesius

Projektledare
SSF Stöldskyddsföreningen

Per Klingvall

Rådgivningschef
SSF Stöldskyddsföreningen

10. Bilagor

1. Grundläggande cybersäkerhet
2. Statistik, polisanmälningar, säkerhetskollen,
3. Utbud av stöd, mer specificerat
4. Enkätfrågor i indexen allmänheten
5. Enkätfrågor i indexen mindre företag
6. Förteckning över sekundärdata