CyberAgent

Co-funded by the European Union

VEILEDNING I GOD PRAKSIS FOR SMÅ OG MELLOMSTORE BEDRIFTER

CYBERAGENT 06.2026

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Arbeidspakke 6: Formidling og utnyttelse

Leveranse 6.4: Veiledning om god praksis for SMB-er

Leder for WP6 – Women4Cyber Foundation

INNHOLD

LISTE OVER TABELLER

INNLEDNING

CyberAgent-prosjektet ble utviklet over tre år i åtte europeiske land: Romania, Belgia, Norge, Spania, Tyrkia, Polen, Litauen og Finland. CyberAgent ble opprettet for å utvikle og teste et modulbasert, tilgjengelig opplæringsprogram i cybersikkerhet for ansatte i SMB-bedrifter, elever i yrkesopplæring og studenter ved høyere utdanningsinstitusjoner. Det sentrale resultatet av dette arbeidet er «Cybersecurity Change Agent»: en opplært, ikke-spesialisert ansatt som fungerer som et internt referansepunkt for bevisstgjøring om cybersikkerhet i sin organisasjon.

Denne veiledningen omsetter prosjektets erfaringer fra gjennomføringen til praktiske råd for SMB-bedrifter. Den forklarer hva rollen som endringsagent innebærer, hvordan man identifiserer og utpeker den rette personen, hvordan man støtter opplæringen og hvordan man sikrer at kjønnsinkludering er integrert i prosessen helt fra starten. En sjekkliste på slutten hjelper SMB-bedrifter med å kontrollere at de rette forholdene er på plass i hvert trinn.

1. HVORFOR CYBERSIKKERHET ER VIKTIG FOR ALLE SMÅ OG MELLOMSTORE BEDRIFTER

Ifølge ENISAs rapport «Threat Landscape 2025» industrialiserer nettkriminelle angrepene sine, noe som gjør SMB-er til attraktive mål uavhengig av størrelse og bransje. De vanligste truslene organisasjoner står overfor i dag, er løsepengevirus, phishing og datainnbrudd. Løsepengevirus og datainnbrudd utgjør til sammen flertallet av cyberkriminalitetshendelser rettet mot organisasjoner i EU, der løsepengevirus står for mer enn 80 % av forbrytelsene. Industrialiseringen av disse angrepene, særlig «Ransomware-as-a-Service»-modellen, har senket terskelen for angripere, noe som gjør selv de minste organisasjonene til levedyktige mål.

Spesielt for SMB-er er konsekvensene av et cyberangrep ikke begrenset til midlertidige forstyrrelser. Ifølge ENISA har cybersikkerhetsangrep alvorlige negative konsekvenser for virksomheten til 90 % av SMB-ene allerede en uke etter at de har funnet sted. Til tross for denne sårbarheten har SMB-er likevel sjelden dedikert IT- eller sikkerhetspersonell, og deres ansatte får sjelden strukturert opplæring i cybersikkerhet. SMB-er i Europa sysselsetter rundt 100 millioner mennesker og står for mer enn halvparten av Europas BNP. Derfor utgjør cybersikkerhetsgapet i SMB-sektoren en økonomisk og samfunnsmessig risiko.

De fleste cyberangrep lykkes på grunn av menneskelige faktorer, som for eksempel å klikke på en phishing-lenke, svake passord eller uverifiserte e-poster. Dette betyr at den første forsvarslinjen ikke er et teknisk verktøy, men en informert og bevisst ansatt som vet hva man skal se etter og hva man skal gjøre når noe går galt. Det er nettopp denne rollen som Cybersecurity Change Agent fyller.

2. ENDRINGSAGENTEN FOR CYBERSIKKERHET

Konseptet «endringsagent for cybersikkerhet» står sentralt i CyberAgent-prosjektet. I dette avsnittet forklares hva rollen innebærer, hvorfor den ble utviklet og hvordan den fungerer i praksis i små og mellomstore bedrifter (SMB).

2.1. HVA ER DET, OG HVORFOR ER DET NØDVENDIG?

SMB-bedrifter er ryggraden i den europeiske økonomien, men de er likevel blant de organisasjonene som er mest utsatt for cybersikkerhetstrusler. I motsetning til store selskaper har de fleste SMB-bedrifter ikke egne IT- eller sikkerhetsavdelinger, og de ansatte får sjelden strukturert opplæring i cybersikkerhet. Dette fører til et vedvarende gap mellom de cybertruslene SMB-bedrifter står overfor og deres evne til å håndtere dem.

CyberAgent-prosjektet og rollen som «Cybersecurity Change Agent» ble utviklet for å bøte på dette gapet ved å bygge opp en annen type kompetanse i eksisterende team. En «Cybersecurity Change Agent» er en opplært, ikke-teknisk ansatt som fungerer som en intern referanseperson for bevissthet om cybersikkerhet, oppmuntrer til tryggere atferd, gjenkjenner vanlige risikoer og implementerer bedre cybersikkerhetspraksis i organisasjonen. Denne rollen vil også fungere som en veiviser for kolleger mot riktig støtte i tilfelle hendelser.

Behovet for denne rollen bekreftes av dataene som ble samlet inn gjennom CyberAgent-pilotprosjektet. I åtte partnerland nådde opplæringen ut til 594 registrerte deltakere, bestående av ansatte i SMB-er, studenter ved høyere utdanningsinstitusjoner og elever i yrkesrettet opplæring. Ansatte i SMB-er blir ofte identifisert som den vanskeligste målgruppen å nå og beholde i utdanningssammenheng, hovedsakelig på grunn av tidsbegrensninger og arbeidsforpliktelser. Likevel gjenspeiler den høye fullføringsgraden blant ansatte i SMB-er den reelle relevansen av bevissthet om cybersikkerhet i deres daglige arbeid.

2.2. HOVEDANSVAR

Cybersikkerhetsendringsagenten har ikke ansvar for å løse cybersikkerhetsproblemer alene. Rollen er bygget opp rundt bevisstgjøring, kommunikasjon og koordinering, og innebærer å være den personen i organisasjonen som holder cybersikkerhet på dagsordenen og hjelper kolleger med å håndtere dette i sitt daglige arbeid. Ingenting av dette krever teknisk ekspertise. Det som kreves, er en person som er betrodd, har et godt nettverk i organisasjonen og er motivert til å gjøre cybersikkerhet til en naturlig del av teamets arbeidsmåte.

Konkret innebærer rollen en rekke gjentakende, enkle aktiviteter som ikke krever mye tid, men som har en betydelig innvirkning på organisasjonens sikkerhetskultur:

- **Å øke bevisstheten regelmessig**. Endringsagenten deler jevnlige bevisstgjøringsmeldinger med kolleger om de vanligste truslene, som phishing-e-poster, svake passord, usikker datahåndtering og mistenkelige lenker, og holder cybersikkerhet synlig uten at det blir en byrde. Dette kan være så enkelt som en månedlig melding i teamchatten, en kort påminnelse før en travel periode eller et notat om en ny type svindel som sirkulerer i bransjen. Formatet er mindre viktig enn at det gjøres jevnlig.

- **Å holde cybersikkerhet på møteagendaen**. Endringsagenten tar opp cybersikkerhetstemaer under teammøter gjennom korte, praktiske diskusjoner. Dette innebærer ikke lange presentasjoner eller formelle opplæringsøkter. En fem minutters samtale om et nylig phishing-forsøk eller en påminnelse om å oppdatere passord er nok til å holde bevisstheten levende og signalisere at cybersikkerhet er et felles ansvar i organisasjonen, ikke noe som delegeres til det tekniske personalet.

- **Oppmuntre til rapportering av hendelser**. Et av de viktigste bidragene fra endringsagenten for cybersikkerhet er å skape en kultur der ansatte føler seg trygge på å rapportere mistenkelige situasjoner, for eksempel en uvanlig e-post, et system som oppfører seg uventet eller en kollega som klikker på noe de ikke burde ha klikket på. Mange cybersikkerhetshendelser eskalerer fordi ansatte ikke rapporterer tidlige varselsignaler av frykt for å bli flau eller få skylden. Endringsagenten bidrar til å normalisere rapporteringen ved å være tilgjengelig og tydelig om prosessen.

- **Støtte ved innføring av** nye medarbeidere. Nye medarbeidere er blant de mest sårbare i enhver organisasjon sett fra et cybersikkerhetsperspektiv, fordi de ikke er kjent med interne prosedyrer, er mer tilbøyelige til å stole på uventede forespørsler og ofte ennå ikke er opplært i grunnleggende sikkerhetsrutiner. Endringsagenten spiller en viktig rolle i å introdusere grunnleggende cybersikkerhet under innføringen, og sikrer at gode vaner etableres fra første dag i stedet for å måtte innarbeides senere.

- **Fungere som et internt kontaktpunkt**. Cybersikkerhetsendringsagenten er den personen kollegene henvender seg til når de har et spørsmål om cybersikkerhet eller er usikre på hva de skal gjøre i en situasjon. Dette innebærer at de vet hvor de kan finne vedkommende, hvem de skal eskalere saken til, og hvordan de kan veilede en kollega mot riktig støtte. I små og mellomstore bedrifter uten dedikert IT-personale fyller denne rollen et tomrom som ellers ville etterlate de ansatte uten et klart referansepunkt.

- **Fremme opplæring og kontinuerlig læring**. Endringsagenten oppmuntrer kolleger til å benytte seg av tilgjengelige opplæringsressurser, inkludert CyberAgent-modulene, og holder seg oppdatert om utviklingen innen cybersikkerhet som er relevant for organisasjonens sektor og virksomhet.
- **Innsamling og videreformidling av tilbakemeldinger**. Endringsagenten samler inn tilbakemeldinger om cybersikkerhetsbekymringer i organisasjonen – om hva de ansatte synes er forvirrende, hvilke retningslinjer som ikke følges, og hvilke risikoer som oppleves som mest presserende – og videreformidler disse innsiktene til ledelsen. Denne tilbakemeldingssløyfen gjør det mulig for organisasjonen å forbedre sin sikkerhetskultur over tid.

Tabell 1. Skille mellom tekniske medarbeideres oppgaver og endringsagentens oppgaver

IT-SPESIALIST (teknisk rolle)	SIKKERHETSFORANDRINGSAGENT (ledelses- og kulturrolle)
Konfigurerer brannmurer og sikkerhetssystemer	Deler skreddersydde bevisstgjøringsmeldinger og sikkerhetsvarsler med kolleger
Håndterer programvareoppdateringer, oppdateringspakker og tekniske konfigurasjoner	Sørger for at cybersikkerhet alltid står på dagsordenen for interne teammøter
Reagerer på pågående cybersikkerhetshendelser og tekniske sikkerhetsbrudd	Oppfordrer kolleger til å rapportere mistenkelige aktiviteter aktivt og åpent

Overvåker nettverkstrafikk, sikkerhetslogger og tekniske samsvarsparametere	Støtter nye ansatte under organisasjonens innkjøringsprosess når det gjelder grunnleggende cybersikkerhetsrutiner
Implementerer tekniske sikkerhetstiltak og administrerer tilgang til infrastrukturen	Innhenter løpende tilbakemeldinger fra ansatte og eskalerer systemiske bekymringer til ledelsen eller IT-avdelingen

3. VALG OG UTNEVNELSE AV EN ENDRINGSAGENT FOR CYBERSIKKERHET

Å identifisere den rette personen til rollen som endringsagent for cybersikkerhet og gi vedkommende forutsetninger for å lykkes, er avgjørende beslutninger når rollen skal implementeres i en organisasjon. CyberAgent-pilotprosjektet viste at rollen fungerer best når den besettes av en person som oppfattes som pålitelig, har god kjennskap til selskapets prosedyrer og støttes av ledelsen. Dette avsnittet gir praktisk veiledning om hvordan man definerer rollen tydelig for langsiktig suksess og hvordan man finner den rette kandidaten.

3.1. HVORDAN FINNE DEN RETTE KANDIDATEN

Ifølge resultatene fra CyberAgent-pilotprosjektet er de mest effektive Cybersecurity Change Agents ikke nødvendigvis de som har teknisk bakgrunn fra før. I de åtte pilotlandene var det de deltakerne fra små og mellomstore bedrifter som engasjerte seg mest aktivt i opplæringen og viste størst potensial, som kombinerte organisasjonsforståelse med kommunikasjonsevner og en genuin motivasjon for å gjøre en forskjell på arbeidsplassen. Basert på erfaringene fra pilotprosjektet er følgende egenskaper ofte med på å sikre suksess i rollen:

- Kjennskap til organisasjonens interne prosesser og praksis for datahåndtering.
- Gode kommunikasjons- og samarbeidsevner.
- Støtte fra ledelsen

Det er viktig å merke seg at rollen ikke krever teknisk eller IT-bakgrunn. Derfor kan ansatte i administrative stillinger, HR, drift og ledelse utføre endringsagentfunksjonen effektivt, forutsatt at de får tilstrekkelig opplæring og støtte. Å fjerne det tekniske kravet er et bevisst designvalg som utvider utvalget av kvalifiserte kandidater betydelig og åpner for kjønnsmangfold, slik pilotprosjektet viste.

Når en kandidat er identifisert, må rollen synliggjøres og legitimeres i organisasjonen. Rollens omfang bør kunngjøres i hele organisasjonen og defineres klart: hva endringsagenten for cybersikkerhet har ansvar for, hvem vedkommende rapporterer til, og hva vedkommende ikke forventes å gjøre.

3.2. IMPLEMENTERING AV ROLLEN

Det neste trinnet er å implementere rollen i en organisasjon. De følgende trinnene bygger direkte på erfaringene fra CyberAgent-pilotprosjektet i partnerlandene og er utformet for å være tilpasset små og mellomstore bedrifter av alle størrelser.

3.2.1. VELG UT OG OPPLÆR CYBERSIKKERHETSENDRINGSAGENTEN

Identifiser den mest egnede personen i organisasjonen din og gi vedkommende tilgang til CyberAgent-opplæringsprogrammet. Programmet består av ni moduler som dekker sikkerhetsprogramledelse (M1), systemadministrasjon (M2), analyseverktøy (M3), sikkerhetsdrift (M4), sikkerhetsstyring og -politikk (M5), cybersikkerhetsplanlegging (M6), risikostyring (M7), forretningskontinuitet (M8) og karriereutvikling innen cybersikkerhet (M9). Disse ni modulene er formelt nedfelt i to offisielle prosjektleveranser: D3.1, som dekker læreplanen for høyere utdanning, og D3.2, som dekker læreplanen for yrkesrettet opplæring. Modulene det henvises til i denne veiledningen samsvarer derfor direkte med innholdet beskrevet i D3.1 og D3.2 og er tilgjengelige via CyberAgent-plattformen uavhengig av deltakernes tilknytning til en institusjon. Videre er læreplanen tilpasset EQF-nivåene 4–6 for ansatte i små og mellomstore bedrifter, og gir grunnleggende ferdigheter og kunnskap innen cybersikkerhet med praktisk anvendelse på tvers av kompetanseområdene teknikk, analyse, risikostyring og organisasjon.

Opplæringen gjennomføres i eget tempo og er tilgjengelig på nettet, noe som betyr at den utvalgte ansatte kan fullføre den fleksibelt ved siden av sine eksisterende arbeidsoppgaver. Når en modul er fullført og kunnskapstesten er bestått med en poengsum på minst 75 %, mottar endringsagenten et kursbevis for den aktuelle modulen. Dette beviset utgjør en formell dokumentasjon av de tilegnede kompetansene og kan brukes til å dokumentere endringsagentens opplæring i organisasjonen.

3.2.2. DEFINER ANSVARSOMRÅDER OG INTEGRER I EKSISTERENDE STRUKTURER

Når opplæringen er i gang eller fullført, bør organisasjonen formelt definere ansvarsområdene til endringsagenten for cybersikkerhet og integrere rollen i eksisterende strukturer. Dette innebærer å bli enige om hva endringsagenten skal gjøre, hvor mye tid vedkommende skal bruke på rollen og hvem vedkommende skal samarbeide med, samt å formidle dette til hele teamet.

Pilotprosjektet viste at rollen som endringsagent for cybersikkerhet er mest bærekraftig når den er knyttet til noe som allerede finnes i organisasjonen, i stedet for å stå isolert. Dette kan innebære å knytte den til et fast punkt på dagsordenen for teammøter eller til en eksisterende struktur for helse, sikkerhet eller samsvar. Målet er å gjøre bevissthet om cybersikkerhet til en naturlig del av det daglige arbeidet og et felles organisatorisk ansvar, ikke en separat aktivitet.

3.2.3. SKAPE INTERN BEVISSTHET OM ROLLEN

Endringsagenten kan ikke fungere effektivt hvis kollegene ikke vet hvem vedkommende er eller hva vedkommende gjør. For å gi den utvalgte medarbeideren den organisatoriske legitimiteten vedkommende trenger for å fungere, er det nødvendig å sende ut en klar internmelding som beskriver rollen og ansvaret, samt å organisere regelmessige møter der medarbeiderne kan stille spørsmål.

Utover den innledende kunngjøringen bør endringsagenten oppmuntres til å holde cybersikkerhet synlig i organisasjonen gjennom regelmessige møter. Dette betyr ikke lange opplæringsøkter eller formelle presentasjoner. I SMB-sammenheng kan dette gjøres i form av korte aktiviteter som er direkte knyttet til situasjoner de ansatte kjenner igjen fra sitt daglige arbeid.

3.2.4. GJENNOMGÅ REGELMESSIG OG OPPRETTHOLD OVER TID

For at rollen som endringsagent for cybersikkerhet skal kunne skape varig effekt, må organisasjonen legge til rette for at den kan fortsette og utvikle seg. Dette innebærer å innføre en evalueringsprosess minst én gang i året for å vurdere hva som fungerer, hvilke mangler som gjenstår, og om endringsagenten trenger ytterligere opplæring eller støtte.

Erfaringene fra pilotprosjektet viser at vedvarende engasjement krever mer enn innledende opplæring. Deltakerne i SMB-sektoren trenger gjennomgående fleksible frister, påminnelser og sporadisk støtte for å opprettholde fremdriften. Å innføre en enkel årlig gjennomgang og sikre at endringsagenten har kontinuerlig tilgang til ressurser, er minimumsvilkårene for å holde rollen effektiv over tid.

4. KJØNNSBALANSE OG INKLUDERING

Cybersikkerhet er fortsatt et av de mest mannsdominerte feltene i den europeiske økonomien. Kvinner utgjør omtrent 20 % av arbeidsstyrken innen cybersikkerhet i hele EU, og deltakelsen i opplæring i cybersikkerhet gjenspeiler den samme ubalansen. På grunn av det eksisterende kompetanse- og talentgapet vil et felt som kun trekker på en brøkdel av den tilgjengelige talentpoolen, slite med å møte den omfanget av etterspørselen som det nåværende trusselbildet krever.

CyberAgent-prosjektet ble utformet med kjønnsinkludering som et eksplisitt mål, ikke som en ettertanke. I et felt hvor kvinner vanligvis utgjør en liten minoritet av opplæringsdeltakerne, er det høye antallet kvinnelige deltakere i pilotprosjektet et betydningsfullt resultat, og det var et produkt av målrettede rekrutteringsstrategier og en inkluderende tilnærming.

4.1. HVORFOR DETTE ER VIKTIG FOR SMB-ER

Spesielt for SMB-er er kjønnsdimensjonen ved cybersikkerhet både et spørsmål om arbeidsstyrken og om organisasjonskulturen. De fleste SMB-er har ikke dedikert cybersikkerhetspersonell. Deres cyberresiliens avhenger av bevisstheten og atferden til alle ansatte, spesielt de som har roller innen administrasjon, HR, økonomi og drift. Derfor utgjør det et sikkerhetshull å ekskludere kvinner fra opplæring i cybersikkerhetsbevissthet.

Samtidig gir rollen som «Cybersecurity Change Agent» en konkret mulighet til å ta tak i kjønnsubalansen innen cybersikkerhet fra innsiden av SMB-bedriftene. Fordi rollen er preget av kommunikasjonsevner, organisasjonsforståelse og styringsfokus snarere enn teknisk ekspertise, passer den godt for et bredt spekter av yrkesprofiler, og den gir kvinner i ikke-tekniske stillinger en anerkjent vei inn i ansvarsområder innen cybersikkerhet som ikke krever karrierebytte eller teknisk utdanning.

4.2. PRAKTISKE TILTAK FOR Å NÅ UT TIL KVINNER OG UNDERREPRESENTERTE GRUPPER

Følgende praktiske tiltak er hentet fra erfaringene fra CyberAgent-pilotprosjektet og er utformet slik at de kan gjennomføres av SMB-bedrifter uansett størrelse.

Det belgiske pilotprosjektet viste at det å kanalisere rekrutteringsarbeidet gjennom nettverk som kvinner allerede har tillit til – for eksempel fagforeninger og nettverk for kvinnelige næringsdrivende – øker kvinnelig deltakelse. I praksis betyr dette at når en SMB skal finne kandidater til rollen som «Cybersecurity Change Agent», bør den aktivt samarbeide med relevante kvinnenettverk innen sin bransje eller region, i stedet for å stole utelukkende på offentlige utlysninger.

Fremstill rollen i lys av organisasjonsmessig innvirkning, ikke teknisk kompetanse. Kvinner i ikke-tekniske roller er mer tilbøyelige til å engasjere seg i opplæring i cybersikkerhet og påta seg rollen som «Change Agent» når rollen presenteres ut fra den organisasjonsmessige verdien den tilfører, snarere enn ut fra tekniske ferdigheter. Rollen kan fremstilles som en som beskytter virksomheten, støtter kolleger og bidrar til styring og ledelse. Språket som brukes i internkommunikasjon, stillingsbeskrivelser og rekrutteringsmateriell er viktig.

5. BESTE PRAKSIS

Å utnevne en endringsagent for cybersikkerhet er et viktig første skritt, men rollen kan bare skape varig innvirkning hvis den opererer innenfor en organisasjonskultur som aktivt støtter den. Følgende beste praksis er utformet for å hjelpe SMB-bedrifter med å skape de rette forholdene for at endringsagenten skal lykkes og for at bevissthet om cybersikkerhet skal bli en naturlig del av hvordan organisasjonen fungerer.

- **Oppmuntre til åpen kommunikasjon**. Ansatte bør føle seg trygge på å rapportere feil, mistenkelige situasjoner eller sikkerhetsbekymringer uten frykt for å bli klandret eller utsatt for forlegenhet. I mange organisasjoner eskalerer cybersikkerhetshendelser nettopp fordi ansatte nøler med å rapportere noe de er usikre på eller føler seg ansvarlige for.

- **Hold det enkelt og integrert i de daglige rutinene**. Bevissthet om cybersikkerhet trenger ikke å ta form av formelle opplæringsøkter eller langvarige workshops. Korte, praktiske påminnelser integrert i eksisterende rutiner er ofte mer effektive enn sporadisk intensiv opplæring. Målet er å gjøre cybersikkerhet til en vane i bakgrunnen, snarere enn en periodisk begivenhet.

- **Dokumenter hvert trinn underveis**. Et av de mest praktiske tiltakene en SMB kan iverksette, er å skrive ned sine grunnleggende cybersikkerhetsrutiner: hvordan passord håndteres, hvordan sensitive data lagres og deles, hva man skal gjøre når en mistenkelig e-post kommer inn, hvem man skal kontakte i tilfelle en hendelse. Dette trenger ikke å være formelle retningslinjedokumenter. En referanse på én side som er tilgjengelig for alle ansatte, er nok.

- **Start på toppen**. Den atferden som forventes av de ansatte, må synlig etterleves av ledere og ledelsen. Hvis ledelsen ikke følger grunnleggende sikkerhetsrutiner, sender det et signal om at disse rutinene er valgfrie. Endringsagentens troverdighet i organisasjonen avhenger delvis av om kulturen rundt dem støtter det de prøver å fremme.

- **Sørg for kontinuerlig bevisstgjøring**. Trusler mot cybersikkerheten utvikler seg stadig, og en enkelt opplæringsøkt blir raskt utdatert. Bevisstgjøring må behandles som en kontinuerlig prosess snarere enn en engangsaktivitet. Dette innebærer regelmessige kontaktpunkter, periodiske oppfriskningskurs og en endringsagent for cybersikkerhet som holder seg informert og kontinuerlig bringer relevant informasjon tilbake til organisasjonen.

5.1. KVALITATIVE TILBAKEMELDINGER FRA DE NASJONALE PILOTPROSJEKTENE

Den kvalitative tilbakemeldingen viser at deltakerne generelt var positive til opplæringen, og mange oppga at det ikke var behov for store forbedringer. De mest gjentatte temaene i de åpne tekstsvarene (D5.3 – Evaluering av opplæringsprogrammet for kompetanseheving av CyberAgent) var: plattformens brukervennlighet, navigasjon eller vurderingsflyt; tekniske problemer med tilgang eller pålitelighet; positiv verdi knyttet til tilgjengelighet, fleksibilitet og bred kunnskap; ønsker om flere praktiske tilfeller, praktiske øvelser eller ekte eksempler fra SMB-sektoren; innholdstetthet, struktur eller differensiering av læringsforløp. Det er verdt å merke seg at det tredje mest nevnte temaet (positiv verdi knyttet til tilgjengelighet, fleksibilitet og bred kunnskap) gjenspeiler anerkjennelse fra deltakere som uttalte at det ikke var behov for forbedringer og som på eget initiativ fremhevet programmets styrker. Dette er et meningsfullt signal: i et åpent tekstfelt som var ment å fange opp kritikk, uttrykte nesten en fjerdedel av de kvalitative svarene tilfredshet med opplæringens tilgjengelighet og bredde.

5.2. HANDLINGSPUNKTER FOR GJENNOMFØRING OG STYRING AV OPPLÆRINGEN I SMB-ER

Den omfattende piloteringen av CyberAgent-plattformen i åtte europeiske land ga viktige innsikter i hvordan små og mellomstore bedrifter tar i bruk og opprettholder kompetanseheving innen cybersikkerhet. Basert på bevisene fra den blandede metoden og hindringene for deltakerne som er dokumentert i den endelige evalueringsrapporten for opplæringen (D5.3), anbefales bedriftsledere å innføre følgende interne ledelsesmessige, tekniske og strategiske tiltak for å optimalisere opplæringens organisatoriske effekt.

Råd om kvalitetsstyring

Læringsmaterialet til CyberAgent inneholder en betydelig mengde operativ og strategisk kunnskap. Ledere bør unngå å tildele hele pensumet på en gang; i stedet vil etablering av en modulbasert tidsplan forhindre kognitiv utmattelse og sikre en jevnere overføring av kompetanse til bedriftens daglige rutiner.

Råd om teknisk integrering

Innledende pilotdata viser at tekniske hindringer ved oppstarten, som forsinkede eller filtrerte e-poster med bekreftelse på plattformregistrering, kan hemme tidlig i bruk. Før brukerregistreringen settes i gang, bør ledelsen koordinere med nettverksfiltrene for å sikre at eksterne e-læringsdomener er fullt ut tillatt, og be de ansatte om å sjekke spam-mappene sine regelmessig.

Råd om strategisk implementering

De nasjonale pilotdataene viste at strategiske moduler på høyere nivå – spesielt M6 (planlegging av cybersikkerhet) og M8 (forretningskontinuitet) – krever solid bakgrunnserfaring for å kunne utnyttes fullt ut. For å maksimere den umiddelbare forretningsverdien bør disse modulene rettes spesielt mot personell med ansvar for ledelse, drift eller forretningsstyring.

5.2.1. ENDRINGSAGENTENS STEMME

Pilotfasen, som samlet inn 272 omfattende svar på spørreundersøkelsen fra åtte europeiske land, avdekket tre tverrgående effekter på målgruppene.

Høy fleksibilitet i gjennomføringen og balanse mellom arbeid og studier

Hele 86,0 % av respondentene var enige eller svært enige i at det asynkrone formatet, der man kan studere i eget tempo, var tilstrekkelig fleksibelt til å integreres sømløst i deres profesjonelle og akademiske timeplaner, noe som gjorde det mulig for ansatte i SMB-bedrifter å balansere kompetanseutvikling med daglige driftsoppgaver.

Metodologisk relevans for ikke-teknisk personell

Resultatene fra pilotprosjektet bekrefter den grunnleggende pedagogiske utformingen av CyberAgent-læreplanen og viser at effektiv cyberresiliens i organisasjonen ikke krever avanserte tekniske ferdigheter eller IT-programmeringskompetanse. I henhold til dataene fra effektvurderingen i D5.3 oppga 77,2 % av deltakerne at opplæringen gjorde dem i stand til å forstå klart hvordan deres spesifikke yrkesroller påvirker og beskytter de daglige sikkerhetsrutinene i en bedrift.

Målbar kunnskapsutvikling fra utgangspunktet for ikke-eksperter

Plattformanalyser viser at 89,3 % av alle deltakerne oppnådde en verifisert økning i sin kunnskap om cybersikkerhet. Avgjørende er at denne utviklingen var mest synlig blant helt nybegynnere: 90,9 % av deltakerne som vurderte sin opprinnelige forståelse som «svært lav» før programmet, rapporterte en avgjørende forbedring i sin kunnskap og selvtillit når det gjelder å gjenkjenne cybersikkerhetsrisikoer i bedriften.

5.2.2. «HVA MAN BØR OG IKKE BØR GJØRE»

Basert på tilbakemeldingene fra pilotlandene angående «differensiering av læringsforløp» presenterer vi anbefalinger for bedrifter:

Tabell 2 «Hva man bør og ikke bør gjøre»

IKKE GJØR (fallgruver for SMB)	ANBEFALT (beste praksis)
Å forvente at en ansatt skal gjennomføre alle 8 modulene innenfor en urealistisk, kort tidsramme (f.eks. én uke eller én måned). Pilotstudier (D5.3) viste at mangel på tid på grunn av daglige arbeidsoppgaver var den største hindringen for ansatte i SMB-bedrifter, noe som førte til en lavere beståttprosent på prøven.	Lage en fleksibel, individuell læringsplan basert på den ansattes behov og tilgjengelighet, ved å anvende prinsippene for mikrolæring. La deltakerne fokusere på moduler som direkte styrker deres spesifikke innflytelse på arbeidsplassen.
Å forvente at den opplærte endringsagenten for cybersikkerhet skal erstatte spesialiserte IT-ingeniører eller selvstendig løse komplekse cyberhendelser. Å overføre forventninger til den tekniske kjerneinfrastrukturen til ikke-teknisk personale skaper stor uklarhet rundt rollen.	Å oppmuntre endringsagenten til å fungere som en intern sikkerhetskoordinator og katalysator for bevisstgjøring. De er mest effektive når de fremmer sikkerhetskultur, sender ut påminnelser om intern opplæring og gir korte oppdateringer under teammøter.
Å la e-læringsprosessen foregå helt uten tilsyn, på autopilot uten innsikt fra bedriften. En enkelt registreringslenke garanterer ikke langsiktig verdi for organisasjonen.	Å benytte det strukturerte overvåkingsrammeverket (for eksempel tabell 3) for å spore milepæler og tildele intern veiledning. Indikasjoner fra pilotevalueringen (D5.3) bekrefter at det å ha en utpekt leder eller mentor har en eksplisitt sammenheng med fullføring av verifiserte tester.

IKKE GJØR (fallgruver for SMB)	ANBEFALT (beste praksis)
Å la selvstudium foregå i fullstendig isolasjon, med fare for at individuelle læringshindringer eller skjulte tekniske problemer forblir ubemerket. Uten interaksjon går nybegynnere ofte i stå og forlater programmet i stillhet når de står fast.	Integrering av selvstudium i eget tempo med proaktive operasjonelle kontaktpunkter, for eksempel korte statuskontroller eller digitale påminnelser. Aktiv ledelsesoppfølging fjerner læringsbarrierer direkte, noe som øker de ansattes motivasjon og fullføringsgraden for kursene.

6. VEIKART FOR Å IMPLEMENTERE ENDRINGSAGENTEN FOR CYBERSIKKERHET

En vellykket implementering av rollen som endringsagent for cybersikkerhet starter lenge før selve utnevnelsen. Å ta seg tid til å vurdere organisasjonens nåværende situasjon, bygge opp intern støtte og definere rollen tydelig fra starten av, øker sjansene for langsiktig suksess betydelig. Følgende trinn er utformet for å veilede SMB-bedrifter gjennom denne forberedelsesfasen på en praktisk måte.

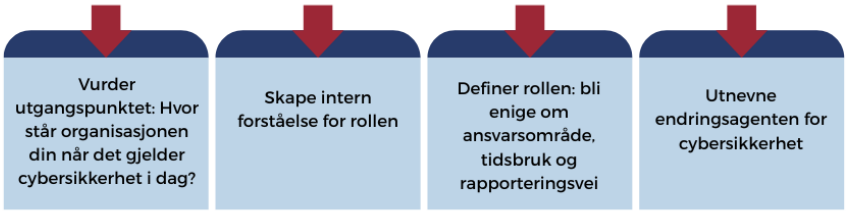
1. Det første trinnet er å vurdere hvor organisasjonen står i dag. Dette innebærer å ta et ærlig blikk på hvilke cybersikkerhetsrutiner som allerede er på plass – eller mangler. Er de ansatte klar over grunnleggende trusler som phishing? Finnes det en prosedyre for å rapportere mistenkelige hendelser? Håndteres sensitive data på en ensartet måte i hele teamet?

2. Det andre trinnet er å skape intern støtte for stillingen. Endringsagenten kan ikke fungere effektivt uten støtte fra ledelsen. Før man velger en kandidat, bør beslutningen om å innføre stillingen diskuteres og vedtas på ledernivå, med en klar forpliktelse til å avsette tid, anerkjenne stillingen formelt og aktivt støtte den som påtar seg oppgaven.

3. Det tredje trinnet er å definere rollen før den besettes. Dette innebærer å bli enige om ansvarsomfanget, forventet tidsbruk og hvordan rollen skal plasseres i den eksisterende organisasjonsstrukturen. Et klart mandat, selv en enkel beskrivelse på ett avsnitt, unngår tvetydighet og gir den fremtidige endringsagenten for cybersikkerhet den legitimiteten vedkommende trenger for å handle.

Først når disse tre trinnene er på plass, er organisasjonen klar til å identifisere og utnevne den rette kandidaten. Det følgende avsnittet skisserer sjekklisten som vil veilede en vellykket implementering av rollen.

Figur1 – Visuell veikart for implementering av endringsagenten for cybersikkerhet



7. SJEKKLISTE

Følgende sjekkliste er ment å brukes til å verifisere om de viktigste forutsetningene for en vellykket implementering av endringsagenten for cybersikkerhet er på plass. Den er basert på erfaringene fra CyberAgent-pilotprosjektet.

7.1. LEDELSE

[ ] Rollen som endringsagent er formelt godkjent og budsjettert

[ ] Det er definert et klart mandat: omfang, tidsbruk og rapporteringslinje

[ ] Utnevnelsen er blitt kommunisert til hele organisasjonen

[ ] Det er planlagt en gjennomgang av rollen innen de neste 12 månedene

[ ] Endringsagenten har avsatt tid i sin timeplan til å utføre rollen

7.2. PERSONALAVDELINGEN

[ ] Utvelgelsesprosessen var åpen for alle, uavhengig av kjønn eller bakgrunn

[ ] Rollen ble kommunisert med tanke på innvirkning på organisasjonen, ikke teknisk kompetanse

[ ] Endringsagentens ansvarsområder er gjenspeilet i stillingsbeskrivelsen eller målene

[ ] Nye ansatte blir presentert for endringsagenten for cybersikkerhet under innkjøringen

[ ] Det føres oversikt over endringsagentens opplæring og sertifiseringer

7.3. ENDRINGSAGENT FOR CYBERSIKKERHET

[ ] Registrert på CyberAgent-plattformen og har avtalt en læringsplan

[ ] Har fullført minst én modul og oppnådd et sertifikat

[ ] Kollegaene vet hvordan de kan komme i kontakt med endringsagenten

[ ] Grunnleggende praksis for cybersikkerhet er dokumentert og tilgjengelig for alle ansatte

[ ] Det er etablert regelmessige bevisstgjøringsaktiviteter (møter, meldinger eller påminnelser)

[ ] Det finnes en klar prosess for kolleger som ønsker å rapportere mistenkelige situasjoner

[ ] Tilbakemeldinger om bekymringer knyttet til cybersikkerhet samles inn og videreformidles regelmessig til ledelsen

8. HVORDAN MÅLE EN VELLYKKET IMPLEMENTERING

Implementeringen av rollen som endringsagent for cybersikkerhet er en kontinuerlig oppgave. Følgende indikatorer kan hjelpe små og mellomstore bedrifter med å vurdere om rollen har en reell innvirkning over tid.

[ ] Antallet ansatte som deltar i bevisstgjøringsaktiviteter om cybersikkerhet har økt siden endringsagenten ble utnevnt

[ ] Cybersikkerhet tas regelmessig opp i teammøter og behandles ikke lenger som et unntaksemne

[ ] Ansatte vet hvem endringsagenten er og føler seg trygge på å henvende seg til vedkommende med spørsmål eller bekymringer

[ ] Antallet rapporterte mistenkelige e-poster, hendelser eller bekymringer har økt

[ ] Endringsagenten har fullført flere opplæringsmoduler siden den første utnevnelsen

[ ] Tilbakemeldinger fra de ansatte om cybersikkerhet i organisasjonen samles inn med jevne mellomrom, og det følges opp

8.1. VEILEDNING FOR LEDERE OM TILPASNING OG TILRETTELEGGING AV MALEN

For å sikre at kompetanseutviklingen til endringsagenten for cybersikkerhet bidrar til langsiktig robusthet i bedriften, er kontinuerlig strukturell overvåking avgjørende. Tabell 3 inneholder en praktisk oppfølgingsmal utformet for ledere i små og mellomstore bedrifter, som kan brukes til å evaluere organisasjonens utgangsnivå før opplæringen og måle konkrete fremskritt i sikkerhetskulturen 6 og 12 måneder etter utnevnelsen.

Ledere bør betrakte denne malen som et dynamisk rammeverk. Avhengig av bedriftens størrelse, bransje og eksisterende infrastruktur oppfordres dere til å tilpasse og utvide denne matrisen:

- **Tilpasning av skalaer**
  Mikro-SMB-er (under 10 ansatte) kan forenkle prosentbaserte måleparametere til direkte antall ansatte for å gjøre oppfølgingen enklere.
- **Utvidelse av indikatorer**
  Bedrifter som opererer i svært digitaliserte eller høyrisikomiljøer, anbefales å legge til målspesifikke rader, for eksempel «% av de ansatte som bruker multifaktorautentisering (MFA)» eller «Gjennomsnittlig responstid på en simulert trussel».
- **Lokalisering**
  Tilpass kolonnen «Anbefalt datakilde» til dine spesifikke interne kommunikasjonskanaler (f.eks. sporing via Slack, avstemninger i MS Teams eller fysiske logger under teambriefinger).

Tabell 3. Mal for oppfølging etter ansettelse for ledere i små og mellomstore bedrifter

Suksessindikator	Enhet / måleskala	Utgangspunkt (før)	Fremgang (6 måneder)	Mål (12 måneder)	Anbefalt datakilde
Ansattes beredskap mot phishing	Andel av de ansatte som føler seg trygge på å håndtere mistenkelige e-poster	%	%	%	Interne pulsundersøkelser eller data fra CyberAgent-plattformen
Hyppighet av møteintegrasjon	Antall teammøter der cybersikkerhet ble tatt opp	Antall	Antall	Antall	Referater/dagsordener fra teammøter
Aktiv rapporteringsrate for hendelser	Antall rapporterte mistenkelige hendelser	Antall / måned	Antall / måned	Antall / måned	Intern sikkerhetslogg eller IT-tilbakemeldingsløyfe
Synlighet for endringsagenten	Andel av de ansatte som vet nøyaktig hvem endringsagenten er	%	%	%	Kort internt spørreskjema
Plattformens fremdrift og engasjement	Antall ansatte som aktivt deltar i mikrolæring	Antall	Antall	Antall	Analysedashbord for CyberAgent-plattformansvarlig

KONKLUSJON

Cybersikkerhet er ikke lenger et anliggende forbeholdt store organisasjoner med egne IT-avdelinger. Ettersom trusselbildet stadig utvikler seg og myndighetenes forventninger til små og mellomstore bedrifter øker, er spørsmålet hvordan de kan forsvare seg med de ressursene de faktisk har til rådighet.

Rollen som «Cybersecurity Change Agent» gir et praktisk og forholdsmessig svar på dette spørsmålet. Det krever ikke å ansette en spesialist, investere i dyre verktøy eller gjennomføre en omfattende omlegging av eksisterende prosesser. Det krever å identifisere den rette personen i organisasjonen, gi vedkommende opplæring og fullmakt til å handle, samt skape forutsetninger for at bevissthet om cybersikkerhet blir en del av hverdagen på arbeidsplassen.

CyberAgent-prosjektet har vist at dette er mulig. I åtte europeiske land fullførte ansatte i SMB-bedrifter uten teknisk bakgrunn opplæringen, påtok seg rollen og begynte å gjøre en forskjell i hvordan organisasjonene deres tilnærmet seg cybersikkerhet. Bevisene er klare: når inngangsbarrieren senkes, når rollen er utformet med utgangspunkt i organisasjonskulturen snarere enn teknisk ekspertise, og når inkludering behandles som et designprinsipp snarere enn en ettertanke, følger resultatene.

Denne veiledningen er en invitasjon til å ta det første skrittet. Veikartet er der. Verktøyene er tilgjengelige. Rollen er innen rekkevidde for alle SMB-bedrifter som er villige til å investere i sine ansatte.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau