Co-funded by the European Union

GHID DE BUNE PRACTICI PENTRU IMM-URI

CYBER AGENT 06.2026

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

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.

www.cyberagents.eu

Pachetul de lucru 6: Diseminare & Exploatare

Livrabilul 6.4: Ghid de bune practici pentru IMM-uri

Lider al PL6 – Fundația Women4Cyber

CUPRINS

LISTA TABELELOR

INTRODUCERE

Proiectul CyberAgent a fost dezvoltat pe parcursul a trei ani în opt țări europene: România, Belgia, Norvegia, Spania, Türkiye, Polonia, Lituania și Finlanda. CyberAgent a fost creat pentru a construi și testa un program de instruire în securitate cibernetică modular și accesibil, destinat angajaților din IMM-uri, cursanților din învățământul profesional și tehnic (VET) și studenților din învățământul superior (HEI). Rezultatul central al acestei activități este Agentul Schimbării în Securitatea Cibernetică: un angajat instruit, nespecialist, care acționează ca punct intern de referință pentru conștientizarea în materie de securitate cibernetică în cadrul organizației sale.

Acest Ghid transpune experiența de implementare a proiectului în îndrumări practice pentru IMM-uri. El explică în ce constă rolul de Agent al Schimbării, cum se identifică și se desemnează persoana potrivită, cum se susține instruirea acesteia și cum se asigură integrarea incluziunii de gen în proces încă de la început. O listă de verificare la final ajută IMM-urile să confirme că sunt îndeplinite condițiile necesare în fiecare etapă.

1. DE CE CONTEAZĂ SECURITATEA CIBERNETICĂ PENTRU FIECARE IMM

Potrivit raportului ENISA Threat Landscape 2025, infractorii cibernetici își industrializează atacurile, transformând IMM-urile în ținte cu valoare ridicată, indiferent de dimensiunea și sectorul lor. Cele mai frecvente amenințări cu care se confruntă astăzi organizațiile sunt ransomware-ul, phishingul și brețele de date. Ransomware-ul și brețele de date reprezintă majoritatea incidentelor de criminalitate informatică care vizează organizațiile din UE, ransomware-ul fiind responsabil pentru peste 80% dintre infracțiuni. Industrializarea acestor atacuri, în special modelul „Ransomware-as-a-Service", a redus barierele pentru atacatori, transformând chiar și cele mai mici organizații în ținte viabile.

În cazul IMM-urilor în special, consecințele unui atac cibernetic nu se limitează la întreruperi temporare. Potrivit ENISA, atacurile cibernetice au un impact negativ grav asupra activității a 90% dintre IMM-uri la o săptămână de la producere. Cu toate acestea, în pofida acestei expuneri, IMM-urile dispun rareori de personal dedicat de IT sau de securitate, iar angajații lor beneficiază rareori de instruire structurată în securitate cibernetică. IMM-urile din Europa angajează aproximativ 100 de milioane de persoane și generează peste jumătate din PIB-ul Europei. Prin urmare, deficitul de securitate cibernetică din sectorul IMM-urilor reprezintă un risc economic și societal.

Majoritatea atacurilor cibernetice reușesc din cauza factorilor umani, precum accesarea unui link de phishing, parolele slabe sau e-mailurile neverificate. Aceasta înseamnă că prima linie de apărare nu este un instrument tehnic, ci un angajat informat și conștient, care știe la ce să fie atent și ce să facă atunci când ceva nu merge bine. Acest rol este exact cel acoperit de Agentul Schimbării în Securitatea Cibernetică.

2. AGENTUL SCHIMBĂRII ÎN SECURITATEA CIBERNETICĂ

Conceptul de Agent al Schimbării în Securitatea Cibernetică se află în centrul proiectului CyberAgent. Această secțiune explică în ce constă rolul, de ce a fost dezvoltat și cum arată în practică în cadrul întreprinderilor mici și mijlocii (IMM-uri).

2.1. CE ESTE ȘI DE CE ESTE NECESAR

IMM-urile reprezintă coloana vertebrală a economiei europene, însă rămân printre cele mai expuse organizații la amenințările de securitate cibernetică. Spre deosebire de companiile mari, majoritatea IMM-urilor nu dispun de departamente dedicate de IT sau de securitate, iar angajații lor beneficiază rareori de instruire structurată în securitate cibernetică. Acest lucru duce la un decalaj persistent între riscurile cibernetice cu care se confruntă IMM-urile și capacitatea pe care o au de a le gestiona.

Proiectul CyberAgent și figura Agentului Schimbării în Securitatea Cibernetică au fost concepute pentru a remedia acest decalaj prin dezvoltarea unui alt tip de capacitate în cadrul echipelor existente. Agentul Schimbării în Securitatea Cibernetică este un angajat instruit, fără pregătire tehnică, care acționează ca referință internă pentru conștientizarea în materie de securitate cibernetică, încurajând comportamente mai sigure, recunoscând riscurile frecvente și implementând practici mai bune de securitate cibernetică în cadrul organizației. Această figură acționează totodată ca ghid pentru colegi, orientându-i către sprijinul adecvat în caz de incidente.

Necesitatea acestui rol este confirmată de dovezile colectate pe parcursul programului-pilot CyberAgent. În cele opt țări partenere, instruirea a ajuns la 594 de participanți înscriși, cuprinzând angajați din IMM-uri, cursanți HEI și VET. Angajații din IMM-uri sunt în mod obișnuit identificați ca fiind cel mai dificil grup-țintă de atras și de menținut în context educațional, în principal din cauza constrângerilor de timp și a responsabilităților profesionale. Cu toate acestea, rata ridicată de finalizare în rândul angajaților din IMM-uri reflectă relevanța reală a conștientizării în materie de securitate cibernetică în activitatea lor de zi cu zi.

2.2. RESPONSABILITĂȚI PRINCIPALE

Agentul Schimbării în Securitatea Cibernetică nu are responsabilitatea de a rezolva singur problemele de securitate cibernetică. Rolul este construit în jurul conștientizării, comunicării și coordonării, fiind persoana din organizație care menține securitatea cibernetică pe agenda și îi ajută pe colegi să o gestioneze în activitatea lor zilnică. Niciunul dintre aceste aspecte nu necesită expertiză tehnică. Ceea ce este necesar este o persoană de încredere, bine conectată în cadrul organizației și motivată să transforme securitatea cibernetică într-o parte firească a modului în care lucrează echipa.

Concret, rolul se traduce printr-un set de activități recurente, ușoare, care nu necesită mult timp, dar care au un impact semnificativ asupra culturii de securitate a organizației:

- **Conștientizarea periodică**. Agentul Schimbării transmite colegilor mesaje periodice de conștientizare privind cele mai frecvente amenințări, precum e-mailurile de phishing, parolele slabe, manipularea nesigură a datelor și linkurile suspecte, menținând securitatea cibernetică vizibilă fără a o transforma într-o povară. Aceasta poate fi la fel de simplă ca un mesaj lunar transmis pe chatul echipei, o scurtă reamintire înainte de o perioadă aglomerată sau o notă despre un nou tip de fraudă care circulă în sector. Formatul contează mai puțin decât consecvența.

- **Menținerea securității cibernetice pe agenda ședințelor**. Agentul Schimbării abordează subiecte de securitate cibernetică în cadrul ședințelor de echipă, prin discuții scurte și practice. Aceasta nu înseamnă prezentări lungi sau sesiuni formale de instruire. O conversație de cinci minute despre o tentativă recentă de phishing sau o reamintire privind actualizarea parolelor este suficientă pentru a menține conștientizarea activă și pentru a semnala că securitatea cibernetică este o responsabilitate organizațională comună, nu ceva delegat personalului tehnic.

- **Încurajarea raportării incidentelor**. Una dintre cele mai importante contribuții ale Agentului Schimbării în Securitatea Cibernetică este crearea unei culturi în care angajații se simt confortabil să raporteze situații suspecte, precum un e-mail neobișnuit, un sistem care se comportă neașteptat sau un coleg care a accesat ceva ce nu ar fi trebuit. Multe incidente de securitate cibernetică se agravează deoarece angajații nu raportează semnele timpurii de avertizare, de teama jenei sau a vinovăției. Agentul Schimbării contribuie la normalizarea raportării, fiind abordabil și explicând clar procesul.

- **Sprijinirea integrării noilor angajați**. Noii angajați se numără printre cei mai vulnerabili membri ai oricărei organizații din perspectiva securității cibernetice, deoarece nu sunt familiarizați cu procedurile interne, sunt mai predispuși să acorde încredere unor solicitări neașteptate și adesea nu au fost încă instruiți în privința practicilor de securitate de bază. Agentul Schimbării joacă un rol important în introducerea noțiunilor de bază de securitate cibernetică în etapa de integrare, asigurând formarea unor obiceiuri bune încă din prima zi, în loc de a fi corectate ulterior.

- **Acționarea ca punct intern de contact**. Agentul Schimbării în Securitatea Cibernetică este persoana la care colegii apelează atunci când au o întrebare legată de securitatea cibernetică sau nu sunt siguri ce să facă într-o anumită situație. Aceasta înseamnă că ei știu unde îl pot găsi, către cine să escaladeze problema și cum să îndrume un coleg către sprijinul potrivit. În IMM-urile fără personal IT dedicat, acest rol acoperă un gol care altfel ar lăsa angajații fără un punct de referință clar.

- **Promovarea instruirii și a învățării continue**. Agentul Schimbării încurajează colegii să utilizeze resursele de instruire disponibile, inclusiv modulele CyberAgent, și se menține la curent cu evoluțiile din peisajul securității cibernetice relevante pentru sectorul și activitățile organizației.

- **Colectarea și escaladarea feedbackului**. Agentul Schimbării colectează feedback privind preocupările de securitate cibernetică din cadrul organizației — ce li se pare angajaților neclar, ce practici nu sunt respectate, ce riscuri sunt resimțite ca fiind cele mai presante — și aduce aceste informații în atenția managementului. Această buclă de feedback este cea care permite organizației să își îmbunătățească în timp cultura de securitate.

Pentru ca aceste activități să se desfășoare fără probleme și pentru a evita confuziile în cadrul întreprinderii, managerii trebuie să facă distincția între sarcinile tehnice IT zilnice și cultura de securitate în sens mai larg. Tabelul 1 conturează această delimitare, indicând ce intră în atribuțiile unui specialist tehnic IT (sau ale unui furnizor extern) și care sunt domeniile coordonate de Agentul de Schimbare în Securitate Cibernetică (non-tehnic).

Tabelul 1. Distincția dintre rolurile Specialistului IT și ale Agentului de Schimbare în Securitate Cibernetică

SPECIALIST IT (Rol tehnic)	AGENT DE SCHIMBARE ÎN SECURITATE CIBERNETICĂ (Rol managerial și cultural)
Configurează și întreține firewall-urile și sistemele de securitate	Transmite colegilor mesaje de conștientizare personalizate și alerte de securitate
Gestionează și implementează actualizările software, patch-urile și configurațiile tehnice	Menține în permanență securitatea cibernetică pe ordinea de zi a ședințelor interne de echipă
Răspunde direct la incidentele cibernetice active și la brețele tehnice de securitate	Încurajează colegii să raporteze în mod activ și transparent activitățile suspecte
Monitorizează traficul de rețea, jurnalele de securitate (logs) și parametrii de conformitate tehnică	Sprijină noii angajați în procesul de integrare organizațională (onboarding) privind igiena cibernetică de bază
Implementează controale tehnice de securitate și gestionează accesul la infrastructură	Colectează feedback continuu de la personal și escaladează problemele sistemice către conducere sau departamentul IT

3. SELECTAREA ȘI DESEMNAREA UNUI AGENT AL SCHIMBĂRII ÎN SECURITATEA CIBERNETICĂ

Identificarea persoanei potrivite pentru rolul de Agent al Schimbării în Securitatea Cibernetică și asigurarea condițiilor pentru reușita acesteia sunt decizii cruciale la implementarea rolului în cadrul unei organizații. Programul-pilot CyberAgent a arătat că rolul funcționează cel mai bine atunci când este ocupat de o persoană percepută ca fiind de încredere, cunoscătoare a procedurilor companiei și susținută de management. Această secțiune oferă îndrumări practice privind modul de a defini clar rolul pentru succesul pe termen lung și modul de a găsi candidatul potrivit.

3.1. CUM SE IDENTIFICĂ CANDIDATUL POTRIVIT

În urma rezultatelor programului-pilot CyberAgent, cei mai eficienți Agenți ai Schimbării în Securitatea Cibernetică nu sunt neapărat cei cu pregătire tehnică anterioară. În cele opt țări participante la pilot, participanții din IMM-uri care s-au implicat cel mai activ în instruire și au demonstrat cel mai mare potențial au fost cei care au combinat înțelegerea organizațională cu abilitățile de comunicare și o motivație autentică de a face diferența la locul de muncă. Pe baza experienței din pilot, următoarele caracteristici tind să susțină succesul în acest rol:

- Familiaritatea cu procesele interne ale organizației și cu practicile de manipulare a datelor.
- Bune abilități de comunicare și interpersonale.
- Sprijin din partea managementului

Important este că rolul nu necesită pregătire tehnică sau IT. Prin urmare, angajații din roluri administrative, din resurse umane, din operațiuni și din management pot îndeplini eficient funcția de Agent al Schimbării, cu condiția de a beneficia de instruire și sprijin adecvate. Eliminarea condiției tehnice este o alegere deliberată de concepție, care lărgește semnificativ rezerva de candidați eligibili și deschide calea către diversitatea de gen, așa cum a demonstrat programul-pilot.

Odată ce un candidat a fost identificat, rolul trebuie făcut vizibil și legitim în cadrul organizației. Domeniul de aplicare al rolului ar trebui anunțat în întreaga organizație și ar trebui definit clar: pentru ce este responsabil Agentul Schimbării în Securitatea Cibernetică, cui îi raportează și ce nu i se cere să facă.

3.2. IMPLEMENTAREA ROLULUI

Următorul pas este implementarea rolului în cadrul unei organizații. Pașii de mai jos se bazează direct pe lecțiile învățate din programul-pilot CyberAgent din țările partenere și sunt concepuți pentru a fi proporționali pentru IMM-uri de orice dimensiune.

3.2.1. SELECTAREA ȘI INSTRUIREA AGENTULUI SCHIMBĂRII ÎN SECURITATEA CIBERNETICĂ

Identificați persoana cea mai potrivită din organizația dumneavoastră și oferiți-i acces la programul de instruire CyberAgent. Programul cuprinde nouă module care acoperă Managementul Programului de Securitate (M1), Administrarea Sistemelor (M2), Instrumente Analitice (M3), Operațiuni de Securitate (M4), Guvernanța și Politica de Securitate (M5), Planificarea Securității Cibernetice (M6), Managementul Riscurilor (M7), Continuitatea Activității (M8) și Dezvoltarea Carierelor în Securitatea Cibernetică (M9). Aceste nouă module sunt formalizate în două livrabile oficiale ale proiectului: D3.1, care acoperă curriculumul HEI, și D3.2, care acoperă curriculumul VET. Modulele la care se face referire pe parcursul acestui Ghid corespund, prin urmare, direct conținutului descris în D3.1 și D3.2 și pot fi accesate prin platforma CyberAgent, indiferent de apartenența instituțională a cursantului. În plus, curriculumul este aliniat la nivelurile 4-6 ale Cadrului European al Calificărilor (CEC) pentru angajații din IMM-uri, oferind competențe și cunoștințe fundamentale de securitate cibernetică, cu aplicabilitate practică în domeniile de competență tehnice, analitice, de management al riscurilor și organizaționale.

Instruirea se desfășoară în ritm propriu și este disponibilă online, ceea ce înseamnă că angajatul selectat o poate parcurge flexibil, în jurul responsabilităților sale profesionale existente. La finalizarea unui modul și promovarea testului de evaluare a cunoștințelor cu un punctaj de cel puțin 75%, Agentul Schimbării primește un Certificat de Finalizare a Cursului pentru modulul respectiv, care constituie o evidență formală a competențelor dobândite și poate fi utilizat pentru a documenta instruirea Agentului Schimbării în cadrul organizației.

3.2.2. DEFINIREA RESPONSABILITĂȚILOR ȘI INTEGRAREA ÎN STRUCTURILE EXISTENTE

Odată ce instruirea este în curs sau finalizată, organizația ar trebui să definească formal responsabilitățile Agentului Schimbării în Securitatea Cibernetică și să integreze rolul în structurile existente. Aceasta înseamnă să se convină asupra a ceea ce va face Agentul Schimbării, cât timp va dedica rolului și cu cine se va coordona, comunicând acest lucru întregii echipe.

Programul-pilot a arătat că rolul de Agent al Schimbării în Securitatea Cibernetică este cel mai sustenabil atunci când este conectat la ceva care există deja în organizație, în loc să funcționeze izolat. Acest lucru ar putea însemna asocierea sa cu un punct recurent de pe agenda ședințelor de echipă sau conectarea sa la o structură existentă de sănătate și securitate în muncă ori de conformitate. Scopul este de a face din conștientizarea securității cibernetice o parte firească a activității de zi cu zi și o responsabilitate organizațională comună, nu o activitate separată.

3.2.3. CONSOLIDAREA CONȘTIENTIZĂRII INTERNE CU PRIVIRE LA ROL

Agentul Schimbării nu poate funcționa eficient dacă colegii nu știu cine este sau ce face. Pentru a-i oferi angajatului selectat legitimitatea organizațională de care are nevoie pentru a-și îndeplini funcția, este necesar să se transmită o comunicare internă clară care să prezinte rolul și responsabilitățile sale și să se organizeze ședințe periodice care să permită angajaților să adreseze întrebări.

Dincolo de anunțul inițial, Agentul Schimbării ar trebui încurajat să mențină securitatea cibernetică vizibilă în organizație prin ședințe periodice. Aceasta nu înseamnă sesiuni lungi de instruire sau prezentări formale. În contextul unui IMM, acest lucru s-ar putea realiza sub forma unor activități scurte, direct legate de situații pe care angajații le recunosc din activitatea lor zilnică.

3.2.4. REVIZUIREA PERIODICĂ ȘI MENȚINEREA ÎN TIMP

Pentru ca rolul de Agent al Schimbării în Securitatea Cibernetică să genereze un impact durabil, organizația trebuie să creeze condițiile pentru ca acesta să continue și să evolueze. Aceasta înseamnă instituirea unui proces de revizuire cel puțin o dată pe an, pentru a evalua ce funcționează, ce lacune persistă și dacă Agentul Schimbării are nevoie de instruire sau sprijin suplimentar.

Dovezile din programul-pilot arată că implicarea susținută necesită mai mult decât instruirea inițială. Participanții din IMM-uri au nevoie în mod constant de termene flexibile, de reamintiri și de sprijin ocazional pentru a-și menține ritmul. Instituirea unei simple revizuiri anuale și asigurarea accesului permanent al Agentului Schimbării la resurse reprezintă condițiile minime pentru menținerea eficacității rolului în timp.

4. ECHILIBRUL DE GEN ȘI INCLUZIUNEA

Securitatea cibernetică rămâne unul dintre cele mai dominate de bărbați domenii din economia europeană. Femeile reprezintă aproximativ 20% din forța de muncă în securitatea cibernetică la nivelul UE, iar participarea la instruirea în securitate cibernetică reflectă același dezechilibru. Din cauza decalajului existent de competențe și de talente, un domeniu care atrage doar o fracțiune din rezerva disponibilă va întâmpina dificultăți în a face față amplorii cererii pe care o impune actualul peisaj al amenințărilor.

Proiectul CyberAgent a fost conceput cu incluziunea de gen ca obiectiv explicit, nu ca o preocupare secundară. Într-un domeniu în care femeile reprezintă de regulă o mică minoritate a participanților la instruire, numărul ridicat de femei participante la pilot este un rezultat semnificativ și a fost produsul unor strategii de informare direcționate și al unei abordări incluzive.

4.1. DE CE CONTEAZĂ PENTRU IMM-URI

În cazul IMM-urilor în special, dimensiunea de gen a securității cibernetice este atât o chestiune de forță de muncă, cât și o chestiune de cultură organizațională. Majoritatea IMM-urilor nu dispun de personal dedicat de securitate cibernetică. Reziliența lor cibernetică depinde de conștientizarea și comportamentul tuturor angajaților, în special al celor din roluri administrative, de resurse umane, financiare și operaționale. Prin urmare, excluderea femeilor de la instruirea de conștientizare în securitate cibernetică reprezintă o vulnerabilitate de securitate.

În același timp, rolul de Agent al Schimbării în Securitatea Cibernetică oferă o oportunitate concretă de a aborda dezechilibrul de gen din securitatea cibernetică din interiorul IMM-urilor. Întrucât rolul este definit prin abilități de comunicare, înțelegere organizațională și gândire orientată spre guvernanță, mai degrabă decât prin expertiză tehnică, el se potrivește unei game largi de profiluri profesionale și oferă femeilor din roluri non-tehnice o cale recunoscută către responsabilitatea în securitate cibernetică, fără a necesita o schimbare de carieră sau o calificare tehnică.

4.2. PAȘI PRACTICI PENTRU A AJUNGE LA FEMEI ȘI LA GRUPURILE SUBREPREZENTATE

Pașii practici de mai jos provin din experiența programului-pilot CyberAgent și sunt concepuți pentru a putea fi implementați de IMM-uri de orice dimensiune.

Programul-pilot din Belgia a demonstrat că direcționarea acțiunilor de informare prin rețele în care femeile au deja încredere, precum asociațiile profesionale și rețelele de femei de afaceri, crește participarea feminină. În practică, aceasta înseamnă că, atunci când un IMM identifică candidați pentru rolul de Agent al Schimbării în Securitatea Cibernetică, ar trebui să implice activ orice rețele profesionale de femei relevante pentru sectorul sau regiunea sa, în loc să se bazeze exclusiv pe anunțuri publice.

Prezentați rolul în termeni de impact organizațional, nu de expertiză tehnică. Femeile din roluri non-tehnice sunt mai predispuse să se implice în instruirea de securitate cibernetică și să preia funcția de Agent al Schimbării atunci când rolul este prezentat prin prisma valorii organizaționale pe care o aduce, mai degrabă decât prin prisma competențelor tehnice. Rolul poate fi prezentat ca unul care protejează afacerea, sprijină colegii și contribuie la guvernanță. Limbajul utilizat în comunicările interne, în fișele de post și în materialele de recrutare contează.

5. BUNE PRACTICI

Desemnarea unui Agent al Schimbării în Securitatea Cibernetică este un prim pas important, dar rolul poate genera un impact durabil doar dacă funcționează în cadrul unei culturi organizaționale care îl susține activ. Bunele practici de mai jos sunt concepute pentru a ajuta IMM-urile să creeze condițiile potrivite pentru ca Agentul Schimbării să reușească și pentru ca conștientizarea în securitate cibernetică să devină o parte firească a modului în care funcționează organizația.

- **Încurajați comunicarea deschisă**. Angajații ar trebui să se simtă confortabil să raporteze greșeli, situații suspecte sau preocupări de securitate, fără teama de a fi învinovățiți sau jenați. În multe organizații, incidentele de securitate cibernetică se agravează tocmai pentru că angajații ezită să raporteze ceva de care nu sunt siguri sau pentru care se simt responsabili.

- **Păstrați simplitatea și integrarea în rutina zilnică**. Conștientizarea în securitate cibernetică nu trebuie să ia forma unor sesiuni formale de instruire sau a unor ateliere îndelungate. Reamintirile scurte și practice, integrate în rutinele existente, sunt adesea mai eficiente decât instruirea intensivă ocazională. Scopul este de a transforma securitatea cibernetică într-un obicei de fundal, mai degrabă decât într-un eveniment periodic.

- **Documentați fiecare etapă a procesului**. Unul dintre cei mai practici pași pe care îi poate face un IMM este să își consemneze în scris practicile de bază de securitate cibernetică: cum sunt gestionate parolele, cum sunt stocate și partajate datele sensibile, ce trebuie făcut când sosește un e-mail suspect, cu cine trebuie luat legătura în caz de incident. Acestea nu trebuie să fie documente formale de politică. Un document de referință de o pagină, accesibil tuturor angajaților, este suficient.

- **Începeți de la vârf**. Comportamentele așteptate de la angajați trebuie să fie modelate vizibil de manageri și de conducere. Dacă managementul nu respectă practicile de securitate de bază, transmite semnalul că aceste practici sunt opționale. Credibilitatea Agentului Schimbării în cadrul organizației depinde, în parte, de măsura în care cultura din jurul său susține ceea ce acesta încearcă să promoveze.

- **Mențineți conștientizarea continuă**. Amenințările de securitate cibernetică evoluează constant, iar o singură sesiune de instruire devine rapid depășită. Conștientizarea trebuie tratată ca un proces continuu, mai degrabă decât ca o activitate unică. Aceasta înseamnă puncte de contact periodice, recapitulări la intervale regulate și un Agent al Schimbării în Securitatea Cibernetică ce se menține informat și aduce în mod constant informații relevante înapoi în organizație.

5.1. CONTRIBUȚII CALITATIVE DIN PROGRAMELE-PILOT NAȚIONALE

Feedbackul calitativ arată că participanții au fost, în general, pozitivi cu privire la instruire, mulți dintre ei afirmând că nu sunt necesare îmbunătățiri majore. Temele cel mai des repetate în răspunsurile cu text liber (D5.3 - Evaluarea Programului de Perfecționare CyberAgent) au fost: utilizabilitatea platformei, navigarea sau fluxul de evaluare; problemele de acces tehnic sau de fiabilitate; valoarea pozitivă privind accesibilitatea, flexibilitatea și cunoștințele generale; solicitări pentru mai multe cazuri practice, laboratoare aplicate sau exemple reale din IMM-uri; densitatea conținutului, structura sau diferențierea parcursului de învățare. Este de remarcat că a treia cea mai menționată temă (valoarea pozitivă privind accesibilitatea, flexibilitatea și cunoștințele generale) reflectă aprecierea participanților care au afirmat că nu sunt necesare îmbunătățiri și au evidențiat spontan punctele forte ale programului. Acesta este un semnal semnificativ: într-un câmp de text liber conceput pentru a surprinde critici, aproape un sfert dintre răspunsurile calitative au exprimat satisfacție față de accesibilitatea și amploarea instruirii.

5.2. PUNCTE DE ACȚIUNE PENTRU IMPLEMENTAREA ȘI GESTIONAREA INSTRUIRII ÎN CADRUL IMM-URILOR

Pilotarea la scară largă a platformei CyberAgent în opt țări europene a oferit informații esențiale despre modul în care întreprinderile mici și mijlocii asimilează și mențin perfecționarea competențelor în domeniul securității cibernetice. Pe baza dovezilor obținute prin metode mixte și a barierelor întâmpinate de cursanți, documentate în raportul final de evaluare a instruirii (D5.3), se recomandă ca managerii întreprinderilor să adopte următoarele puncte de acțiune interne — manageriale, tehnice și strategice — pentru a optimiza impactul organizațional al instruirii.

Recomandări privind managementul calității

Materialele de instruire CyberAgent conțin un volum substanțial de cunoștințe operaționale și strategice. Managerii ar trebui să evite alocarea întregii programe deodată; în schimb, stabilirea unui calendar modular previne suprasolicitarea cognitivă și asigură o tranziție mai lină a competențelor în activitățile zilnice ale companiei.

Recomandări privind integrarea tehnică

Datele inițiale din etapa de pilotare au evidențiat că dificultățile tehnice de integrare (onboarding), precum întârzierea sau filtrarea e-mailurilor de confirmare a înregistrării pe platformă, pot îngreuna adoptarea timpurie. Înainte de a lansa înscrierea utilizatorilor, conducerea ar trebui să configureze filtrele de rețea astfel încât domeniile externe de e-learning să fie permise integral (allowlisting) și să recomande personalului să verifice folderele de spam.

Recomandări privind implementarea strategică

Datele din pilotarea națională au arătat că modulele strategice de nivel superior – în special M6 (Planificarea securității cibernetice) și M8 (Continuitatea activității) – necesită o experiență solidă prealabilă pentru a fi valorificate pe deplin. Pentru a maximiza valoarea imediată pentru afacere, aceste module ar trebui direcționate cu precădere către personalul cu responsabilități manageriale, operaționale sau de guvernanță a afacerii.

5.2.1. VOCEA AGENTULUI DE SCHIMBARE

Etapa de pilotare, care a agregat 272 de răspunsuri complete la chestionare din opt țări europene, a evidențiat trei tipuri de impact transversal asupra grupurilor-țintă.

Flexibilitate ridicată a livrării și echilibru între muncă și studiu

Un procent semnificativ de 86,0% dintre respondenți au fost de acord sau total de acord că formatul asincron, în ritm propriu, a fost suficient de flexibil pentru a fi integrat fără dificultăți în programul lor profesional și academic, permițând angajaților din IMM-uri să îmbine dezvoltarea competențelor cu sarcinile operaționale zilnice.

Relevanță metodologică pentru personalul non-tehnic

Rezultatele pilotării validează concepția educațională de bază a programei CyberAgent, demonstrând că o reziliență cibernetică organizațională eficace nu necesită competențe tehnice avansate sau cunoștințe de programare IT. Conform datelor de evaluare a impactului din D5.3, 77,2% dintre participanți au declarat că instruirea le-a permis să înțeleagă clar modul în care rolurile lor profesionale specifice influențează și protejează practicile de securitate cotidiene din cadrul unei întreprinderi.

Progres măsurabil al cunoștințelor de la niveluri inițiale de non-experți

Analizele platformei arată că 89,3% dintre participanți au înregistrat o creștere verificată a cunoștințelor de securitate cibernetică. Esențial este faptul că acest progres a fost cel mai vizibil în rândul începătorilor absoluți: 90,9% dintre cursanții care și-au evaluat nivelul inițial de înțelegere ca fiind „Foarte scăzut” înainte de program au raportat o îmbunătățire decisivă a cunoștințelor și a încrederii în a recunoaște riscurile cibernetice din mediul corporativ.

5.2.2. „CE TREBUIE ȘI CE NU TREBUIE FĂCUT” (DO'S AND DON'TS)

Pe baza feedbackului din țările-pilot privind „diferențierea parcursurilor de învățare”, prezentăm următoarele recomandări pentru companii:

Tabelul 2. „Ce trebuie și ce nu trebuie făcut” (Do's and Don'ts)

DE EVITAT (Capcane frecvente în IMM-uri)	RECOMANDAT (Bune practici)
Așteptarea ca un angajat să parcurgă toate cele 8 module într-un interval de timp nerealist și comprimat (de ex., o săptămână sau o lună). Studiile-pilot (D5.3) au arătat că lipsa timpului, cauzată de responsabilitățile zilnice de la locul de muncă, a fost principala barieră pentru angajații din IMM-uri, ducând la o rată mai scăzută de promovare a testelor.	Crearea unui program de învățare flexibil și individualizat, în funcție de nevoile și disponibilitatea angajatului, aplicând principiile micro-învățării (micro-learning). Permiteți cursanților să se concentreze pe modulele care le îmbunătățesc direct domeniul specific de impact la locul de muncă.
Așteptarea ca Agentul de Schimbare în Securitate Cibernetică, după instruire, să înlocuiască ingineria IT specializată sau să rezolve în mod independent incidente cibernetice complexe. Transferarea responsabilităților privind infrastructura tehnică de bază către personal non-tehnic generează o ambiguitate accentuată a rolurilor.	Încurajarea Agentului de Schimbare să acționeze ca un coordonator intern de securitate și un catalizator al conștientizării. Aceștia sunt cei mai eficienți atunci când promovează cultura de securitate, transmit memento-uri privind instruirile interne și susțin scurte informări în cadrul ședințelor de echipă.
Lăsarea procesului de e-learning complet nemonitorizat, pe „pilot automat”, fără vizibilitate la nivelul companiei. Un simplu link de înregistrare nu garantează valoare organizațională pe termen lung.	Utilizarea unui cadru structurat de monitorizare (precum Tabelul 3) pentru urmărirea etapelor-cheie și desemnarea unui mentorat intern. Indiciile din evaluarea pilotării (D5.3) confirmă că existența unui manager sau mentor desemnat se corelează în mod explicit cu finalizarea verificată a testelor.
Permiterea desfășurării studiului independent în izolare totală, cu riscul ca blocajele individuale de învățare sau dificultățile tehnice ascunse să rămână nesesizate. Fără interacțiune, începătorii absoluți deseori stagnează și abandonează în tăcere programul atunci când se blochează.	Integrarea studiului în ritm propriu cu puncte de contact operaționale proactive, precum scurte verificări de tip „pulse check” sau memento-uri digitale. Implicarea activă a conducerii elimină direct barierele de învățare, sporind motivația angajaților și rata de finalizare a cursurilor.

6. FOAIE DE PARCURS PENTRU IMPLEMENTAREA AGENTULUI SCHIMBĂRII ÎN SECURITATEA CIBERNETICĂ

Implementarea cu succes a rolului de Agent al Schimbării în Securitatea Cibernetică începe cu mult înainte de desemnarea propriu-zisă. Alocarea timpului necesar pentru a evalua situația actuală a organizației, pentru a construi sprijin intern și pentru a defini clar rolul încă de la început crește semnificativ șansele de succes pe termen lung. Pașii de mai jos sunt concepuți pentru a ghida practic IMM-urile pe parcursul acestei etape de pregătire.

1. Primul pas este evaluarea situației actuale a organizației. Aceasta înseamnă o analiză onestă a practicilor de securitate cibernetică deja existente sau a absenței lor. Sunt angajații conștienți de amenințările de bază, precum phishingul? Există o procedură de raportare a incidentelor suspecte? Sunt datele sensibile gestionate în mod consecvent în cadrul echipei?

2. Al doilea pas este construirea sprijinului intern pentru rol. Agentul Schimbării nu poate funcționa eficient fără susținerea managementului. Înainte de a selecta un candidat, decizia de a introduce rolul ar trebui discutată și convenită la nivel de management, cu un angajament clar de a aloca timp, de a recunoaște formal rolul și de a sprijini activ persoana care îl preia.

3. Al treilea pas este definirea rolului înainte de a-l ocupa. Aceasta înseamnă să se convină asupra domeniului de responsabilități, a timpului așteptat a fi alocat și a modului în care rolul se va încadra în structura organizațională existentă. Un mandat clar, fie și o simplă descriere de un paragraf, evită ambiguitatea și oferă viitorului Agent al Schimbării în Securitatea Cibernetică legitimitatea de care are nevoie pentru a acționa.

Abia după ce acești trei pași sunt îndepliniți, organizația este pregătită să identifice și să desemneze candidatul potrivit. Secțiunea următoare prezintă lista de verificare care va ghida implementarea cu succes a rolului.

7. LISTĂ DE VERIFICARE

Lista de verificare de mai jos este menită a fi utilizată pentru a confirma dacă sunt îndeplinite condițiile-cheie pentru o implementare de succes a Agentului Schimbării în Securitatea Cibernetică. Ea se bazează pe lecțiile învățate din programul-pilot CyberAgent.

7.1. MANAGEMENT

[ ] Rolul de Agent al Schimbării a fost convenit formal și bugetat

[ ] A fost definit un mandat clar: domeniu de aplicare, timp alocat și linie de raportare

[ ] Desemnarea a fost comunicată întregii organizații

[ ] A fost programată o revizuire a rolului în următoarele 12 luni

[ ] Agentul Schimbării are timp dedicat în programul său pentru a îndeplini rolul

7.2. RESURSE UMANE

[ ] Procesul de selecție a fost deschis tuturor persoanelor, indiferent de gen sau de proveniență

[ ] Rolul a fost comunicat în termeni de impact organizațional, nu de expertiză tehnică

[ ] Responsabilitățile Agentului Schimbării au fost reflectate în fișa postului sau în obiectivele sale

[ ] Noii angajați sunt prezentați Agentului Schimbării în Securitatea Cibernetică în etapa de integrare

[ ] Se păstrează o evidență a instruirii și a certificărilor Agentului Schimbării

7.3. AGENTUL SCHIMBĂRII ÎN SECURITATEA CIBERNETICĂ

[ ] Înregistrat pe platforma CyberAgent și a convenit un parcurs de învățare

[ ] A finalizat cel puțin un modul și a obținut un certificat

[ ] Colegii știu cum să ia legătura cu Agentul Schimbării

[ ] Practicile de bază de securitate cibernetică sunt documentate și accesibile întregului personal

[ ] Există puncte de contact periodice de conștientizare (ședințe, mesaje sau reamintiri)

[ ] Există un proces clar prin care colegii pot raporta situații suspecte

[ ] Feedbackul privind preocupările de securitate cibernetică este colectat și escaladat periodic către management

8. CUM SE MĂSOARĂ O IMPLEMENTARE DE SUCCES

Implementarea rolului de Agent al Schimbării în Securitatea Cibernetică este un angajament continuu. Indicatorii de mai jos pot ajuta IMM-urile să evalueze dacă rolul are un impact real în timp.

[ ] Numărul angajaților care participă la activități de conștientizare în securitate cibernetică a crescut de la desemnarea Agentului Schimbării

[ ] Securitatea cibernetică este abordată periodic în ședințele de echipă și nu mai este tratată ca un subiect excepțional

[ ] Angajații știu cine este Agentul Schimbării și se simt confortabil să i se adreseze cu întrebări sau preocupări

[ ] Numărul de e-mailuri, incidente sau preocupări suspecte raportate a crescut

[ ] Agentul Schimbării a finalizat module de instruire suplimentare de la desemnarea sa inițială

[ ] Feedbackul personalului privind securitatea cibernetică din organizație este colectat periodic și valorificat

8.1. ÎNDRUMĂRI MANAGERIALE PENTRU ADAPTAREA ȘI PERSONALIZAREA MODELULUI (TEMPLATE)

Pentru a vă asigura că perfecționarea Agentului de Schimbare în Securitate Cibernetică se transformă într-o reziliență corporativă pe termen lung, monitorizarea structurală continuă este esențială. Tabelul 3 oferă un model practic de monitorizare, conceput pentru managerii de IMM-uri, în vederea evaluării nivelului organizațional de referință înainte de instruire și a măsurării progresului concret al culturii de securitate la 6 și 12 luni după desemnare.

Managerii ar trebui să trateze acest model ca pe un cadru dinamic. În funcție de dimensiunea întreprinderii, sectorul operațional și infrastructura existentă, sunteți încurajați să adaptați și să extindeți această matrice:

- **Personalizarea scalelor**
  Microîntreprinderile (sub 10 angajați) pot simplifica indicatorii exprimați procentual, transformându-i în numărări directe de angajați, pentru a menține ușurința monitorizării.
- **Extinderea indicatorilor**
  Întreprinderilor care operează în medii puternic digitalizate sau cu risc ridicat li se recomandă să adauge rânduri specifice obiectivelor, precum „% din personal care utilizează autentificarea cu mai mulți factori (MFA)” sau „Timpul mediu de răspuns la o amenințare simulată”.

- **Localizarea**
  Aliniați coloana „Sursa de date recomandată” la canalele de comunicare interne specifice (de ex., monitorizare prin Slack, sondaje în MS Teams sau jurnale fizice completate în timpul ședințelor de echipă).

Tabelul 3. Model de monitorizare post-desemnare pentru managerii de IMM-uri

Indicator de succes	Unitate / Scală de măsură	Nivel de referință (Înainte)	Progres (6 luni)	Țintă (12 luni)	Sursa de date recomandată
Gradul de pregătire a angajaților față de phishing	% din personal care gestionează cu încredere e-mailurile suspecte	%	%	%	Sondaj intern de tip „pulse” sau date din platforma CyberAgent
Frecvența integrării în ședințe	Numărul de ședințe de echipă în care a fost abordată securitatea cibernetică	Număr	Număr	Număr	Procesele-verbale / ordinea de zi a ședințelor de echipă
Rata activă de raportare a incidentelor	Numărul de incidente suspecte documentate și raportate	Număr / lună	Număr / lună	Număr / lună	Jurnalul intern de incidente de securitate sau bucla de feedback IT
Vizibilitatea Agentului de Schimbare	% din personal care știe cu exactitate cine este Agentul de Schimbare	%	%	%	Chestionar intern scurt
Angajamentul față de progresul pe platformă	Numărul de angajați implicați activ în micro-învățare	Număr	Număr	Număr	Tabloul de bord de analiză al managerului din platforma CyberAgent

CONCLUZIE

Securitatea cibernetică nu mai este o preocupare rezervată organizațiilor mari, cu departamente IT dedicate. Pe măsură ce peisajul amenințărilor continuă să evolueze, iar așteptările de reglementare față de IMM-uri cresc, întrebarea este cum se pot apăra acestea cu resursele pe care le au efectiv la dispoziție.

Rolul de Agent al Schimbării în Securitatea Cibernetică oferă un răspuns practic și proporțional la această întrebare. El nu necesită angajarea unui specialist, investiția în instrumente costisitoare sau revizuirea proceselor existente. Necesită identificarea persoanei potrivite din cadrul organizației, asigurarea instruirii și a mandatului de a acționa și crearea condițiilor pentru ca conștientizarea în securitate cibernetică să devină parte a vieții profesionale de zi cu zi.

Proiectul CyberAgent a demonstrat că acest lucru este realizabil. În opt țări europene, angajați din IMM-uri fără pregătire tehnică au finalizat instruirea, au preluat rolul și au început să facă o diferență în modul în care organizațiile lor abordau securitatea cibernetică. Dovezile sunt clare: atunci când bariera de intrare este redusă, când rolul este prezentat în jurul culturii organizaționale, mai degrabă decât al expertizei tehnice, și când incluziunea este tratată ca un principiu de concepție, nu ca o preocupare secundară, rezultatele apar.

Acest Ghid este o invitație de a face primul pas. Foaia de parcurs există. Instrumentele sunt disponibile. Rolul este la îndemâna oricărui IMM dispus să investească în oamenii săi.

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