Co-funded by the European Union

GEROSIOS PRAKTIKOS GAIRĖS MAŽOMS IR VIDUTINIO DYDŽIO ĮMONĖMS (MVĮ)

CYBER AGENT 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

6 darbo paketas: Sklaida ir rezultatų naudojimas

6.4 rezultatas: Gerosios praktikos gairės mažų ir vidutinio dydžio įmonėms (MVĮ)

6 darbo paketo (DP6) lyderis – Women4Cyber Foundation

TURINYS

LENTELIŲ SĄRAŠAS

ĮVADAS

„CyberAgent“ projektas buvo vykdomas trejus metus aštuoniose Europos šalyse: Rumunijoje, Belgijoje, Norvegijoje, Ispanijoje, Turkijoje, Lenkijoje, Lietuvoje ir Suomijoje. Iniciatyvos tikslas – sukurti ir išbandyti modulinę bei lengvai prieinamą kibernetinio saugumo mokymo programą, skirtą MVĮ darbuotojams, profesinio mokymo įstaigų ir aukštųjų mokyklų studentams. Pagrindinis šios veiklos rezultatas – kibernetinio saugumo pokyčių agento vaidmuo. Tai atitinkamus mokymus išklausęs darbuotojas (ne IT srities specialistas), kuris organizacijoje tampa pagrindiniu kontaktiniu asmeniu, į kurį kreipiamasi kibernetinio saugumo sąmoningumo klausimais.

Šiose gairėse pateikiama sukaupta projekto įgyvendinimo patirtis perkeliama į praktines rekomendacijas, skirtas MVĮ. Jame paaiškinama pokyčių agento vaidmens esmė, patariama, kaip parinkti bei paskirti tinkamiausią kandidatą, kaip organizuoti jo mokymą ir užtikrinti, kad įtraukties bei lyčių pusiausvyros principai būtų integruoti nuo pat pradžių. Gairių pabaigoje pateiktas kontrolinis sąrašas padeda įmonėms įvertinti, ar kiekviename etape yra sudarytos visos reikiamos sąlygos.

1. KODĖL KIBERNETINIS SAUGUMAS YRA SVARBUS KIEKVIENAI MVĮ

Remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) 2025 m. kibernetinių grėsmių apžvalga (angl. Threat Landscape), kibernetiniai nusikaltėliai savo veiksmus vykdo pramoniniu mastu, todėl mažos ir vidutinės įmonės (MVĮ) tampa itin vertingais taikiniais, nepriklausomai nuo jų dydžio ar veiklos sektoriaus. Šiuo metu dažniausiai pasitaikančios grėsmės, su kuriomis susiduria organizacijos, yra išpirkos reikalaujančios programinės įrangos atakos (angl. ransomware), duomenų viliojimas (angl. phishing) ir duomenų saugumo pažeidimai. Būtent išpirkos reikalaujančios programinės įrangos atakos ir duomenų saugumo pažeidimai sudaro didžiąją dalį prieš ES organizacijas nukreiptų kibernetinių nusikaltimų, o vien tik išpirkos reikalaujančios programinės įrangos atvejai sudaro daugiau nei 80 % visų incidentų. Šių atakų industrializacija, o ypač modelis „išpirkos reikalaujanti programinė įranga kaip paslauga“ (angl. Ransomware-as-a-Service), sumažino kliūtis programiškiams, todėl net ir pačios mažiausios įmonės tapo realiais taikiniais.

MVĮ sektoriuje kibernetinių atakų pasekmės toli gražu neapsiriboja tik laikinais veiklos sutrikimais. ENISA duomenimis, praėjus savaitei po kibernetinio saugumo incidento, net 90 % nukentėjusių MVĮ patiria rimtą neigiamą poveikį savo verslui. Visgi, nepaisant kylančių grėsmių, MVĮ retai turi specializuotų IT ar saugumo specialistų, o įmonių darbuotojams retai rengiami sistemingi kibernetinio saugumo mokymai. Kadangi Europos MVĮ dirba apie 100 milijonų žmonių ir šis sektorius sukuria daugiau nei pusę Europos BVP, kibernetinio saugumo spragos ir sąmoningumo trūkumas MVĮ sektoriuje kelia rimtą ekonominę bei visuomeninę riziką.

Didžioji dalis kibernetinių atakų būna sėkmingos dėl žmogiškojo veiksnio – pavyzdžiui, paspaudus apgaulingą nuorodą, naudojant silpnus slaptažodžius ar atidarius nepatikrintus el. laiškus. Tai rodo, kad pirmoji gynybos linija yra ne techninės priemonės, o informuotas ir sąmoningas darbuotojas, gebantis atpažinti grėsmes bei žinantis, kaip elgtis incidento atveju. Būtent šią funkciją organizacijoje atlieka kibernetinio saugumo pokyčių agentas.

2. KIBERNETINIO SAUGUMO POKYČIŲ AGENTAS

Kibernetinio saugumo pokyčių agento koncepcija yra esminė „CyberAgent“ projekto ašis. Šioje dalyje paaiškinama šio vaidmens esmė, jo atsiradimo priežastys bei praktinis pritaikymas mažose ir vidutinėse įmonėse (MVĮ).

2.1. KAS TAI YRA IR KODĖL ŠIS VAIDMUO REIKALINGAS

Mažos ir vidutinės įmonės (MVĮ) yra Europos ekonomikos pagrindas, tačiau jos išlieka vienos pažeidžiamiausių organizacijų kibernetinių grėsmių atžvilgiu. Skirtingai nuo didžiųjų bendrovių, dauguma MVĮ neturi specializuotų IT ar saugumo padalinių, o jų darbuotojai retai dalyvauja sisteminguose kibernetinio saugumo mokymuose. Dėl to atsiranda nuolatinis atotrūkis tarp kibernetinių rizikų, su kuriomis susiduria MVĮ, ir jų turimų pajėgumų šioms rizikoms suvaldyti.

„CyberAgent“ projektu ir kibernetinio saugumo pokyčių agento vaidmeniu siekiama užpildyti šią spragą ir padėtų esamoms komandoms įgyti naujų kompetencijų. Kibernetinio saugumo pokyčių agentas – tai atitinkamus mokymus išklausęs darbuotojas (ne techninio profilio specialistas), veikiantis kaip pagrindinis vidinis asmuo kibernetinio saugumo sąmoningumo klausimais. Jis skatina saugesnį elgesį, padeda atpažinti dažniausiai pasitaikančias rizikas ir diegti pažangesnes kibernetinio saugumo praktikas organizacijoje. Be to, šis asmuo prireikus nukreipia kolegas, kur ieškoti reikiamos pagalbos įvykus incidentui.

Šio vaidmens būtinybę patvirtina projekto „CyberAgent“ pilotinių mokymų metu surinkti duomenys. Aštuoniose šalyse partnerėse mokymuose užsiregistravo 594 dalyviai: MVĮ darbuotojai, aukštųjų mokyklų studentai ir profesinio mokymo įstaigų studentai. MVĮ darbuotojai dažnai įvardijami kaip viena sudėtingiausių tikslinių grupių, kurią sunku pritraukti ir išlaikyti mokymosi procese – tam didžiausios įtakos turi laiko trūkumas bei tiesioginės darbo atsakomybės. Visgi aukštas mokymo programos baigimo rodiklis tarp MVĮ darbuotojų rodo, kad kibernetinio saugumo sąmoningumas yra itin aktualus jų kasdienėje veikloje.

2.2. PAGRINDINĖS ATSAKOMYBĖS

Kibernetinio saugumo pokyčių agentas nėra vienintelis asmuo, atsakingas už visų saugumo problemų sprendimą. Šis vaidmuo grindžiamas sąmoningumo didinimu, komunikacija ir veiksmų koordinavimu – pokyčių agentas užtikrina, kad kibernetinis saugumas išliktų įmonės darbotvarkėje, ir padeda kolegoms vadovautis saugumo principais kasdienėje veikloje. Šiam vaidmeniui nereikia specifinių techninių žinių. Svarbiausia, kad asmuo būtų patikimas, turėtų gerą ryšį su komanda ir būtų motyvuotas siekti, kad kibernetinis saugumas taptų natūralia kasdienio darbo dalimi.

Kasdienėje veikloje šis vaidmuo susideda iš periodinių, nesudėtingų veiklų, kurios nereikalauja daug laiko, tačiau daro didelę įtaką organizacijos saugumo kultūrai:

- **Reguliarus sąmoningumo didinimas.** Pokyčių agentas nuolat dalijasi su kolegomis informacija apie dažniausiai pasitaikančias grėsmes, pavyzdžiui, duomenų viliojimo (angl. phishing) laiškus, silpnus slaptažodžius, nesaugų duomenų tvarkymą ar įtartinas nuorodas. Tai leidžia išlaikyti temos aktualumą neapsunkinant darbuotojų. Informavimas gali vykti paprastais būdais: kas mėnesį išsiunčiant žinutę komandos susirašinėjimo kanale, pateikiant trumpą priminimą prieš intensyvų darbų laikotarpį arba atkreipiant dėmesį į sektoriuje plintančias naujas sukčiavimo schemas. Šiuo atveju nuoseklumas yra daug svarbesnis už pačią pranešimo formą.

- **Kibernetinio saugumo integravimas į susirinkimų darbotvarkę.** Pokyčių agentas inicijuoja trumpas, praktiškas diskusijas kibernetinio saugumo temomis komandos susirinkimų metu. Tam nereikia rengti ilgų pristatymų ar oficialių mokymų. Pakanka penkių minučių pokalbio apie neseniai pastebėtą bandymą sukčiauti arba priminimo atsinaujinti slaptažodžius. Tai padeda palaikyti darbuotojų budrumą ir siunčia signalą, kad kibernetinis saugumas yra bendra visos organizacijos atsakomybė, o ne tik techninių darbuotojų reikalas.

- **Skatinimas pranešti apie incidentus.** Vienas svarbiausių pokyčių agento uždavinių – kurti tokią organizacinę kultūrą, kurioje darbuotojai nebijotų pranešti apie įtartinas situacijas: keistus el. laiškus, neįprastą sistemos veikimą ar atvejus, kai kolega netyčia paspaudė nesaugią nuorodą. Daugelis kibernetinių incidentų atneša daug didesnių nuostolių būtent todėl, kad darbuotojai iš gėdos ar baimės būti apkaltinti laiku nepraneša apie pirmuosius įspėjamuosius ženklus. Pokyčių agentas padeda normalizuoti šį procesą, būdamas atviras bendravimui ir aiškiai paaiškindamas veiksmų eigą.

- **Pagalba integruojant naujus darbuotojus (angl. onboarding).** Žiūrint iš kibernetinio saugumo perspektyvos, naujai pasamdyti darbuotojai yra viena pažeidžiamiausių grupių organizacijoje, nes jie dar nežino vidinių procedūrų, labiau linkę pasitikėti netikėtomis užklausomis ir dažnai nėra išklausę bazinių saugumo mokymų. Pokyčių agentas atlieka svarbų vaidmenį supažindindamas naujokus su esminiais saugumo principais jų adaptacijos laikotarpiu. Taip užtikrinama, kad saugūs įpročiai būtų ugdomi nuo pirmos dienos, užuot klaidas taisius vėliau.

- **Vaidmuo organizacijos viduje (kontaktinis asmuo).** Kibernetinio saugumo pokyčių agentas yra tas žmogus, į kurį kolegos kreipiasi iškilus klausimams ar dvejojant, kaip elgtis tam tikroje situacijoje. Darbuotojai žino, kur jį rasti, kam perduoti informaciją ir kaip gauti reikiamą pagalbą. MVĮ, kurios neturi dedikuotų IT specialistų, šis vaidmuo užpildo kritinę spragą, apsaugodamas darbuotojus nuo nežinomybės ir aiškaus orientyro stokos.

- **Mokymų ir nuolatinio tobulėjimo skatinimas.** Pokyčių agentas skatina kolegas naudotis turimais mokymosi ištekliais, įskaitant „CyberAgent“ modulius, taip pat pats domisi kibernetinio saugumo aktualijomis bei tendencijomis, kurios yra svarbios įmonės veiklai ir sektoriui.

- **Grįžtamojo ryšio rinkimas ir perdavimas vadovybei.** Pokyčių agentas fiksuoja organizacijoje kylančias problemas: kas darbuotojams atrodo neaišku, kokių saugumo taisyklių nesilaikoma, kokios rizikos atrodo didžiausios, ir dalijasi šiomis įžvalgomis su vadovybe. Šis grįžtamojo ryšio ciklas leidžia įmonei nuosekliai ir efektyviai stiprinti savo saugumo kultūrą.

1 lentelė. Techninių darbuotojų ir pokyčių agento funkcijų atskyrimas

IT SPECIALISTAS (Techninė vaidmuo)	KIBERNETINIO SAUGUMO POKYČIŲ AGENTAS (Vadybinis ir organizacinės kultūros vaidmuo)
Konfigūruoja užkardas (ugniasienes) ir saugumo sistemas	Platina kolegoms pritaikytus sąmoningumo didinimo pranešimus ir įspėjimus apie saugumo grėsmes
Valdo programinės įrangos atnaujinimus, pataisas ir technines konfigūracijas	Užtikrina, kad kibernetinio saugumo temos būtų įtrauktos į komandos susirinkimų darbotvarkes
Reaguoja į aktyvius kibernetinius incidentus ir techninius saugumo pažeidimus	Skatina kolegas aktyviai ir atvirai pranešti apie įtartiną veiklą
Stebi tinklo srautą, saugumo žurnalus (įrašus) ir techninės atitikties parametrus	Supažindina naujus darbuotojus su bazine kibernetine higiena jų adaptacijos (įsiliejimo į organizaciją) laikotarpiu
Diegia technines saugumo priemones ir valdo prieigos prie infrastruktūros teises	Nuolat renka darbuotojų grįžtamąjį ryšį ir perduoda sistemines problemas vadovams arba IT skyriui

3. KIBERNETINIO SAUGUMO POKYČIŲ AGENTO ATRANKA IR SKYRIMAS

Tinkamo asmens parinkimas kibernetinio saugumo pokyčių agento vaidmeniui ir reikiamų sąlygų jo sėkmingai veiklai sudarymas yra esminiai sprendimai, diegiant šią funkciją organizacijoje. Vykdant „CyberAgent“ pilotinius mokymus paaiškėjo, šios pareigos duoda daugiausiai naudos, kai jas prisiima darbuotojas, kuriuo pasitikima, kuris puikiai išmano įmonės vidaus procesus ir jaučia stiprų vadovų palaikymą. Šiame skyriuje pateikiamos praktinės rekomendacijos, kaip rasti tinkamiausią kandidatą ir aiškiai apibrėžti jo funkcijas, siekiant ilgalaikio rezultato.

3.1. KAIP PARINKTI TINKAMĄ KANDIDATĄ

Remiantis „CyberAgent“ pilotinių mokymų rezultatais, efektyviausiai kibernetinio saugumo pokyčių agento funkcijas atlieka nebūtinai tie darbuotojai, kurie turi techninį išsilavinimą ar ankstesnės šios srities patirties. Visose aštuoniose projekto šalyse aktyviausiai mokymuose dalyvavę ir didžiausią potencialą pademonstravę MVĮ atstovai buvo tie, kurie gebėjo suderinti įmonės procesų išmanymą, puikius komunikacinius įgūdžius bei nuoširdžią motyvaciją kurti teigiamus pokyčius savo darbo aplinkoje. Remiantis sukaupta patirtimi, šią sėkmę dažniausiai lemia šios savybės bei aplinkybės:

- Įmonės vidaus procesų ir duomenų tvarkymo praktikos išmanymas.
- Geri bendravimo ir tarpasmeninių santykių įgūdžiai.
- Stiprus vadovų palaikymas.

Svarbu pabrėžti, kad šiam vaidmeniui nėra būtinas techninis ar IT srities pasirengimas. Todėl administravimo, žmogiškųjų išteklių, veiklos valdymo (operacijų) ar vadovybės padalinių darbuotojai gali sėkmingai atlikti pokyčių agento funkcijas, jei jiems suteikiami atitinkami mokymai bei parama. Techninio reikalavimo atsisakymas yra apgalvotas programos struktūros sprendimas, kuris, kaip parodė pilotiniai mokymai, reikšmingai išplečia potencialių kandidatų ratą ir sudaro palankesnes sąlygas lyčių įvairovei užtikrinti.

Parinkus tinkamą kandidatą, šis vaidmuo organizacijoje turi įgyti oficialų statusą bei matomumą. Informacija apie naująsias funkcijas turėtų būti pristatyta visai organizacijai, tiksliai apibrėžiant veiklos ribas: už ką kibernetinio saugumo pokyčių agentas yra atsakingas, kam jis yra pavaldus ir kokių užduočių iš jo nereikėtų tikėtis.

3.2. POKYČIŲ AGENTO VAIDMENS ĮDIEGIMAS ORGANIZACIJOJE

Parinkus kandidatą, prasideda kitas etapas – šio vaidmens įgyvendinimas įmonėje. Toliau nurodyti veiksmai tiesiogiai remiasi „CyberAgent“ pilotinių mokymų metu šalyse partnerėse įgyta patirtimi. Jie parengti taip, kad būtų proporcingi ir lengvai pritaikomi bet kokio dydžio MVĮ.

3.2.1. KIBERNETINIO SAUGUMO POKYČIŲ AGENTO ATRANKA IR MOKYMAS

Parinkite tinkamiausią darbuotoją savo organizacijoje ir suteikite jam prieigą prie „CyberAgent“ mokymo programos. Programą sudaro devyni moduliai: Saugumo programų valdymas (M1), Sistemų administravimas (M2), Analitiniai įrankiai (M3), Saugumo operacijos (M4), Saugumo valdysena ir politika (M5), Kibernetinio saugumo planavimas (M6), Rizikos valdymas (M7), Veiklos tęstinumas (M8) ir Profesinis įgalinimas kibernetinio saugumo srityje (M9).

Šių devynių modulių turinys yra oficialiai patvirtintas dviejuose projekto rezultatuose (dokumentuose): D3.1, kuriame pateikiama aukštojo mokslo studijų programa, ir D3.2, skirtame profesinio mokymo programai. Todėl šiame dokumente minimi moduliai tiesiogiai atitinka D3.1 ir D3.2 dokumentuose aprašytą turinį, o prieiga prie jų teikiama „CyberAgent“ platformoje, nepriklausomai nuo to, kokio tipo įstaigai besimokantysis priklauso. Be to, MVĮ darbuotojams skirta mokymo programa yra suderinta su Europos kvalifikacijų sąrangos (EKS) 4–6 lygiais; ji suteikia bazinių kibernetinio saugumo žinių bei įgūdžių, kurie praktiškai pritaikomi techninėje, analitinėje, rizikos valdymo ir organizacinėje kompetencijų srityse.

Mokymai vyksta internetu ir yra pritaikyti mokytis savu tempu, todėl pasirinktas darbuotojas gali juos lanksčiai derinti su tiesioginėmis darbo pareigomis. Sėkmingai baigęs modulį ir surinkęs ne mažiau kaip 75 % per žinių patikrinimo testą, pokyčių agentas gauna atitinkamo modulio baigimo pažymėjimą. Šis dokumentas oficialiai patvirtina įgytas kompetencijas ir gali būti naudojamas darbuotojo kvalifikacijai įmonėje įforminti.

3.2.2. ATSAKOMYBIŲ APIBRĖŽIMAS IR INTEGRAVIMAS Į ESAMAS STRUKTŪRAS

Prasidėjus arba pasibaigus mokymams, organizacija turėtų oficialiai apibrėžti kibernetinio saugumo pokyčių agento atsakomybes ir integruoti šį vaidmenį į esamas struktūras. Tai apima susitarimą dėl agento funkcijų, šiam vaidmeniui skiriamo laiko bei bendradarbiavimo su kitais darbuotojais, taip pat visos komandos informavimą apie šiuos pokyčius.

Pilotiniai mokymai parodė, kad kibernetinio saugumo pokyčių agento vaidmuo yra tvariausias tuomet, kai jis integruojamas į jau veikiančius organizacijos procesus, užuot egzistavęs izoliuotai. Pavyzdžiui, šias užduotis galima įtraukti kaip nuolatinį komandos susirinkimų klausimą arba susieti su darbuotojų saugos, sveikatos bei atitikties užtikrinimo procesais. Pagrindinis tikslas – užtikrinti, kad kibernetinis sąmoningumas taptų natūralia kasdienio darbo dalimi ir bendra įmonės atsakomybe, o ne atskira, papildoma veikla.

3.2.3. VIDINIO SĄMONINGUMO APIE ŠĮ VAIDMENĮ DIDINIMAS

Pokyčių agentas negalės dirbti efektyviai, jei kolegos nežinos, kas jis yra ir kokias funkcijas atlieka. Siekiant suteikti pasirinktam darbuotojui reikiamą oficialų statusą bei autoritetą sėkmingai veiklai vykdyti, būtina išplatinti aiškų vidinį pranešimą, kuriame pristatomas šis vaidmuo bei atsakomybės, ir rengti reguliarius susitikimus, skirtus darbuotojų klausimams atsakyti.

Po pradinio pranešimo pokyčių agentą reikėtų skatinti ir toliau palaikyti kibernetinio saugumo temos aktualumą organizacijoje per reguliarius susitikimus. Tai nereiškia, kad būtina rengti ilgus mokymus ar oficialius pristatymus. Mažų ir vidutinių įmonių (MVĮ) kontekste tam puikiai tinka trumpos užduotys ar diskusijos, tiesiogiai susietos su situacijomis, su kuriomis darbuotojai nuolat susiduria kasdieniame darbe.

3.2.4. REGULIARI PERŽIŪRA IR ILGALAIKIS PALAIKYMAS

Siekdama užtikrinti ilgalaikį kibernetinio saugumo pokyčių agento veiklos poveikį, organizacija turi sudaryti sąlygas šiam vaidmeniui plėtotis ir evoliucionuoti. Tai reiškia, kad bent kartą per metus būtina numatyti veiklos peržiūros procesą, skirtą įvertinti, kas veikia efektyviai, kokios spragos dar liko ir ar pokyčių agentui reikalingi papildomi mokymai bei parama.

Pilotinių mokymų rezultatai rodo, kad ilgalaikiam įsitraukimui užtikrinti vien pradinių mokymų nepakanka. Mažų ir vidutinių įmonių (MVĮ) atstovams nuolat reikalingi lankstesni terminai, priminimai ir periodinė pagalba, padedanti palaikyti reikiamą veiklos tempą. Paprasto metinio vertinimo numatymas ir nuolatinės prieigos prie išteklių užtikrinimas pokyčių agentui yra minimalios sąlygos, būtinos šio vaidmens efektyvumui išlaikyti ilgalaikėje perspektyvoje.

4. LYČIŲ BALANSAS IR ĮTRAUKTIS

Kibernetinis saugumas tebėra viena iš sričių Europos ekonomikoje, kurioje labiausiai dominuoja vyrai. Moterys sudaro maždaug 20 % visos ES kibernetinio saugumo darbo jėgos, o dalyvavimo šios srities mokymuose rodikliai rodo tokią pačią nelygybę. Esant dabartiniam talentų stygiui, šiam sektoriui bus itin sunku patenkinti augantį poreikį, kylantį dėl vis sudėtingesnės kibernetinių grėsmių aplinkos, jei ir toliau bus remiamasi tik nedidele dalimi turimo visuomenės potencialo.

Projektas „CyberAgent“ iš pat pradžių buvo rengiamas keliant aiškų lyčių įtraukties tikslą, o ne paliekant tai kaip vėlesnį ar papildomą aspektą. Sektoriuje, kuriame moterys paprastai sudaro nedidelę mokymų dalyvių dalį, gausus jų įsitraukimas į pilotinių mokymų veiklas yra reikšmingas pasiekimas. Šį rezultatą lėmė tikslinės auditorijos pasiekimo strategijos ir kryptingas įtraukties temos pabrėžimas.

4.1. KODĖL TAI SVARBU MVĮ SEKTORIUJE

Mažų ir vidutinių įmonių (MVĮ) atveju lyčių aspektas kibernetinio saugumo srityje yra susijęs tiek su žmogiškaisiais ištekliais, tiek su organizacine kultūra. Dauguma MVĮ neturi dedikuotų kibernetinio saugumo specialistų, todėl jų kibernetinis atsparumas priklauso nuo visų darbuotojų sąmoningumo ir elgsenos – ypač tų, kurie dirba administracijos, personalo valdymo, finansų ir operacijų skyriuose. Dėl šios priežasties moterų neįtraukimas į kibernetinio saugumo mokymus organizacijoje atveria kritinę saugumo spragą.

Kartu kibernetinio saugumo pokyčių agento vaidmuo suteikia realią galimybę spręsti lyčių disbalanso problemą pačių MVĮ viduje. Kadangi šiai funkcijai atlikti labiau reikalingi komunikaciniai įgūdžiai, organizacijos procesų supratimas ir strateginis valdymo mąstymas, o ne gilios techninės žinios, šis vaidmuo puikiai tinka įvairių sričių specialistams. Tai atveria oficialų kelią moterims, dirbančioms netechninėse pozicijose, prisiimti atsakomybę už kibernetinį saugumą nekeičiant karjeros krypties ir neįgyjant IT kvalifikacijos.

4.2. PRAKTINIAI ŽINGSNIAI, SKIRTI PASIEKTI MOTERIS IR MAŽIAU ATSTOVAUJAMAS GRUPES

Belgijoje vykdyti pilotiniai mokymai parodė, kad tikslinės auditorijos pasiekimas per tinklus, kuriais moterys jau pasitiki (pavyzdžiui, profesines asociacijas ir verslo moterų klubus), didina moterų įsitraukimą. Todėl, ieškodama kandidatų šiam vaidmeniui, įmonė turėtų aktyviai bendradarbiauti su jos sektoriui ar regionui aktualiais moterų profesiniais tinklais, o ne pasikliauti vien tik bendrais viešais skelbimais.

Pristatant šias pareigas, svarbu akcentuoti jų įtaką organizacijai, o ne technines žinias. Netechninį darbą dirbančios moterys labiau linkusios dalyvauti kibernetinio saugumo mokymuose ir prisiimti pokyčių agento atsakomybę, kai ši funkcija pristatoma per jos kuriamą vertę įmonei, o ne per techninius reikalavimus. Šį vaidmenį geriausia apibūdinti kaip **skirtą verslui saugoti**, kolegoms padėti ir prie bendro organizacijos valdymo prisidėti. Dėl šios priežasties vidinėje komunikacijoje, pareigybių aprašymuose ir atrankos medžiagoje naudojama kalba bei akcentai turi lemiamą reikšmę.

5. GEROSIOS PRAKTIKOS

Kibernetinio saugumo pokyčių agento paskyrimas yra svarbus pirmasis žingsnis, tačiau šis vaidmuo užtikrins ilgalaikį poveikį tik tuomet, jei bus integruotas į jį aktyviai palaikančią organizacinę kultūrą. Toliau pateikiamos rekomendacijos yra skirtos padėti MVĮ sukurti tinkamas sąlygas pokyčių agento sėkmei ir užtikrinti, kad kibernetinis sąmoningumas taptų natūralia kasdienės įmonės veiklos dalimi.

- **Skatinkite atvirą komunikaciją.** Darbuotojai turėtų jaustis saugiai ir laisvai pranešdami apie klaidas, įtartinas situacijas ar saugumo problemas, nebijodami kaltinimų ar gėdos. Daugelyje organizacijų kibernetinio saugumo incidentai išauga į rimtas krizes būtent todėl, kad darbuotojai dvejoja pranešti apie dalykus, dėl kurių nėra tikri arba jaučiasi kalti.

- **Supaprastinkite procesus ir integruokite juos į kasdienę rutiną.** Kibernetinio saugumo sąmoningumo ugdymas nebūtinai turi vykti oficialių mokymų ar ilgų seminarų forma. Trumpi, praktiški priminimai, įtraukti į įprastus procesus, dažnai yra efektyvesni už retus, bet intensyvius kursus. Tikslas – paversti kibernetinį saugumą nuolatiniu įpročiu, o ne proginiu įvykiu.

- **Aprašykite ir aiškiai pateikite taisykles.** Vienas praktiškiausių žingsnių, kurį gali žengti MVĮ, yra pagrindinių kibernetinio saugumo taisyklių aprašymas: kaip valdomi slaptažodžiai, kaip saugomi ir bendrinami jautrūs duomenys, ką daryti gavus įtartiną el. laišką ir su kuo susisiekti įvykus incidentui. Tai neprivalo būti oficialios, sudėtingos strategijos – pakanka vieno puslapio atmintinės, prieinamos visiems darbuotojams.

- **Pradėkite nuo vadovų pavyzdžio.** Elgseną, kurios tikimasi iš darbuotojų, savo pavyzdžiu privalo demonstruoti vadovai ir įmonės lyderiai. Jei vadovai nesilaiko pagrindinių saugumo taisyklių, komandai siunčiamas signalas, kad šios praktikos yra neprivalomos. Pokyčių agento autoritetas organizacijoje iš dalies priklauso nuo to, ar aplinka palaiko vertybes, kurias jis bando skiepyti.

- **Užtikrinkite sąmoningumo tęstinumą.** Kibernetinio saugumo grėsmės nuolat kinta, todėl vienkartiniai mokymai greitai praranda aktualumą. Sąmoningumo ugdymą reikėtų vertinti kaip nenutrūkstamą procesą, o ne kaip vienkartinį projektą. Tai apima reguliarų grįžtamąjį ryšį, periodinį žinių atnaujinimą bei pokyčių agento įsitraukimą – jis turi sekti naujienas ir nuolat dalytis aktualia informacija su organizacija.

5.1. KOKYBINĖS ĮŽVALGOS IŠ NACIONALINIŲ PILOTINIŲ MOKYMŲ

Kokybinio vertinimo rezultatai rodo, kad dalyviai mokymus įvertino teigiamai, o daugelis jų pažymėjo, kad jokių esminių patobulinimų nereikia. Atviruose atsakymuose (D5.3 – „CyberAgent“ kvalifikacijos kėlimo mokymo programos vertinimas) dažniausiai pasikartojo šios temos: platformos patogumas, navigacija ir vertinimo procesas; techninės prieigos ar sistemos patikimumo problemos; teigiamas programos prieinamumo, lankstumo ir visapusiškų žinių įvertinimas; pageidavimai pateikti daugiau praktinių užduočių, interaktyvių laboratorinių darbų ar realių MVĮ pavyzdžių; turinio tankumas, struktūra arba mokymo programos pritaikymas pagal poreikius (diferencijavimas).

Verta pažymėti, kad trečia pagal dažnumą tema (teigiamas prieinamumo, lankstumo ir visapusiškų žinių įvertinimas) atspindi tų dalyvių pripažinimą, kurie teigė, kad programos tobulinti nereikia, ir savo iniciatyva išskyrė jos stiprybes. Tai reikšmingas rodiklis: atviro teksto laukelyje, kuris paprastai yra skirtas konstruktyviai kritikai, beveik ketvirtadalis kokybinių atsakymų atskleidė pasitenkinimą mokymų prieinamumu ir suteikiamo turinio visapusiškumu.

5.2. REKOMENDUOJAMI VEIKSMAI MOKYMAMS ĮGYVENDINTI IR VALDYTI MVĮ

Didelio masto platformos „CyberAgent“ pilotiniai mokymai aštuoniose Europos šalyse suteikė vertingų įžvalgų apie tai, kaip mažos ir vidutinės įmonės (MVĮ) įsisavina bei palaiko kibernetinio saugumo kvalifikacijos kėlimo procesus. Remiantis mišrių tyrimo metodų duomenimis ir besimokančiųjų iššūkiais, užfiksuotais galutinėje mokymų vertinimo ataskaitoje (D5.3), įmonių vadovams rekomenduojama imtis šių vidaus valdymo, techninių bei strateginių veiksmų, kad būtų pasiektas maksimalus mokymų poveikis organizacijai.

Kokybės valdymo rekomendacijos

„CyberAgent“ mokomoji medžiaga apima didelės apimties praktines, teorines ir strategines žinias. Vadovams patariama nepaskirti visos mokymo programos iš karto – sudarius nuoseklų tvarkaraštį pagal modulius, pavyks išvengti perdegimo ir užtikrinti sklandesnę naujų gebėjimų integraciją į kasdienę įmonės veiklą.

Techninės integracijos rekomendacijos

Pilotinių mokymų duomenys parodė, kad techniniai nesklandumai pradžioje (pavyzdžiui, vėluojantys arba saugumo sistemų blokuojami platformos registracijos el. laiškai) gali sulėtinti darbuotojų įsitraukimą į mokymus. Prieš pradedant darbuotojų registraciją, vadovai turėtų suderinti nustatymus su tinklo administratoriais, kad būtų užtikrinta prieiga prie el. mokymosi platformos, bei paraginti darbuotojus pasitikrinti nepageidaujamo pašto (šlamšto) aplankus.

Strateginio diegimo rekomendacijos

Pilotinių mokymų duomenys atskleidė, kad aukštesnio lygio strateginiams moduliams – ypač M6 (Kibernetinio saugumo planavimas) ir M8 (Veiklos tęstinumas) – medžiagai perprasti reikalinga profesinė patirtis. Siekiant užtikrinti greitą ir tiesioginę vertę verslui, šiuos modulius tikslingiausia skirti darbuotojams, atliekantiems vadovaujamąsias, operacines arba įmonės valdymo funkcijas.

5.2.1. POKYČIŲ AGENTO ĮŽVALGOS IR PATIRTIS

Pilotinių mokymų metu aštuoniose Europos šalyse iš viso buvo surinkti 272 apklausos atsakymai atskleidė tris pagrindinius (horizontaliuosius) poveikius tikslinėms grupėms.

Didelis mokymų lankstumas ir darbo bei studijų derinimas

Net 86,0 % respondentų pritarė arba visiškai pritarė teiginiui, kad asinchroninis, savarankiškam mokymuisi pritaikytas formatas buvo pakankamai lankstus, kad jį būtų galima sklandžiai suderinti su darbo ir studijų grafikais. Tai leido MVĮ darbuotojams sėkmingai ugdyti kompetencijas neapleidžiant kasdienių tiesioginių pareigų.

Metodologinė vertė netechninių pozicijų darbuotojams

Pilotinių mokymų rezultatai patvirtina pagrindinę „CyberAgent“ mokymo programos koncepciją ir įrodo, kad efektyviam įmonės kibernetiniam atsparumui užtikrinti nebūtini pažangūs techniniai ar IT programavimo įgūdžiai. Remiantis ataskaitoje D5.3 pateiktais poveikio vertinimo duomenimis, 77,2 % dalyvių nurodė, kad šie mokymai padėjo jiems aiškiai suprasti, kaip jų konkrečios profesinės funkcijos daro įtaką kasdienėms saugumo praktikoms įmonėje ir prisideda prie jos apsaugos.

Išmatuojamas žinių augimas pradedančiųjų grupėje

Platformos analitiniai duomenys rodo, kad 89,3 % visų dalyvių akivaizdžiai pagerino savo kibernetinio saugumo žinias. Svarbu pažymėti, kad šis augimas buvo ryškiausias tarp visiškų pradedančiųjų: 90,9 % besimokančiųjų, kurie prieš programos pradžią savo žinias vertino kaip „labai žemas“, nurodė sulaukę esminio žinių proveržio ir pradėję labiau pasitikėti savo jėgomis atpažįstant įmonėms kylančias kibernetines grėsmes.

5.2.2. REKOMENDUOTINI IR NEREKOMENDUOTINI VEIKSMAI

Atsižvelgdami į pilotiniuose mokymuose dalyvavusių šalių grįžtamąjį ryšį dėl mokymo programos pritaikymo pagal individualius poreikius (diferencijavimo), pateikiame šias rekomendacijas įmonėms:

2 lentelė. Rekomenduotini ir nerekomenduotini veiksmai

KO NEDARYTI (MVĮ klaidos)	REKOMENDUOJAMA (Geriausios praktikos)
Tikėtis, kad darbuotojas išklausys visus 8 modulius per nerealiai trumpą laiką (pavyzdžiui, per savaitę ar mėnesį). Vertinimo ataskaitos (D5.3) parodė, kad laiko trūkumas dėl kasdienių tiesioginių užduočių buvo pagrindinė kliūtis MVĮ darbuotojams, lėmusi žemesnius testų išlaikymo rodiklius.	Sudaryti lankstų, individualų mokymosi grafiką, pritaikytą prie darbuotojo poreikių bei užimtumo, remiantis mikromokymosi (angl. micro-learning) principais. Svarbu leisti besimokantiesiems susitelkti į tuos modulius, kurie tiesiogiai didina jų veiklos efektyvumą konkrečioje darbo vietoje.
Tikėtis, kad paruoštas kibernetinio saugumo pokyčių agentas pakeis kvalifikuotus IT inžinierius arba savarankiškai spręs sudėtingus kibernetinius incidentus. Esminių techninės infrastruktūros valdymo lūkesčių perkėlimas netechninį darbą dirbantiems darbuotojams sukelia vaidmenų ir atsakomybių painiavą.	Skatinti pokyčių agentą veikti kaip vidiniam saugumo koordinatoriui ir sąmoningumo didinimo katalizatoriui. Šis vaidmuo yra efektyviausias tuomet, kai darbuotojas prisideda prie saugumo kultūros formavimo, teikia vidinius priminimus apie mokymus ir trumpai pristato naujienas komandos susirinkimų metu.
Palikti el. mokymosi procesą visiškai savieigai, be jokios priežiūros ar įmonės kontrolės. Vien tik registracijos nuorodos išsiuntimas negarantuoja ilgalaikės vertės organizacijai.	Naudoti struktūruotą stebėjimo sistemą (pavyzdžiui, pateiktą tolesniame skyriuje) pažangai sekti bei paskirti vidinį mentorių. Pilotinių mokymų vertinimo įžvalgos (D5.3) patvirtina, kad paskirto vadovo ar mentoriaus priežiūra tiesiogiai koreliuoja su sėkmingu testų išlaikymu ir programos baigimu.
Leisti savarankiškoms studijoms vykti visiškoje izoliacijoje, rizikuojant, kad individualios mokymosi kliūtys ar nepaslėpti techniniai nesklandumai liks neišspręsti. Neturėdami galimybės pasikonsultuoti, visiški pradedantieji dažnai praranda motyvaciją ir, susidūrę su sunkumais, tyliai nutraukia programą.	Suderinti savarankišką mokymąsi su proaktyviu palaikymu – pavyzdžiui, trumpais tarpiniais statuso patikrinimais ar priminimais. Aktyvus vadovų įsitraukimas tiesiogiai padeda šalinti mokymosi kliūtis, didina darbuotojų motyvaciją ir gerina kursų baigimo rodiklius.

6. KIBERNETINIO SAUGUMO POKYČIŲ AGENTO ĮDIEGIMO GAIRĖS

Sėkmingas kibernetinio saugumo pokyčių agento vaidmens įgyvendinimas prasideda dar gerokai prieš patį paskyrimą. Skirdama laiko esamos situacijos įvertinimui, vidinio palaikymo užtikrinimui ir tiksliam funkcijų apibrėžimui nuo pat pradžių, organizacija reikšmingai padidina ilgalaikės sėkmės tikimybę. Toliau pateikti žingsniai yra skirti praktiškai padėti MVĮ įveikti šį pasirengimo etapą.

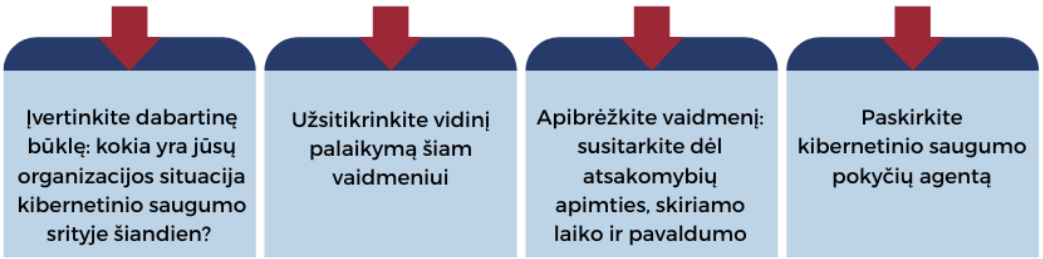
1. **Pirmasis žingsnis – įvertinti dabartinę organizacijos situaciją.** Tai reiškia, kad reikia objektyviai apžvelgti jau taikomas arba trūkstamas kibernetinio saugumo praktikas. Ar darbuotojai atpažįsta pagrindines grėsmes, pavyzdžiui, sukčiavimą el. paštu (angl. phishing)? Ar įmonėje numatyta pranešimų apie įtartinus incidentus tvarka? Ar visa komanda vienodai saugiai elgiasi su jautriais duomenimis?

2. **Antrasis žingsnis – užsitikrinti vidinį palaikymą šiam vaidmeniui.** Pokyčių agentas negalės dirbti efektyviai be vadovų paramos. Dar prieš pasirenkant kandidatą, sprendimas įvesti šią funkciją turi būti apsvarstytas ir patvirtintas vadovų lygmeniu, prisiimant aiškų įsipareigojimą skirti tam laiko, oficialiai pripažinti šį vaidmenį bei aktyviai palaikyti jį prisiimantį darbuotoją.

3. **Trečiasis žingsnis – aiškiai apibrėžti vaidmenį dar prieš paskiriant žmogų.** Tai apima susitarimą dėl atsakomybių apimties, mokymuisi bei veiklai numatomo laiko ir šios funkcijos vietos esamoje organizacinėje struktūroje. Aiškūs įgaliojimai – net ir paprasto vienos pastraipos aprašymo pavidalu – padeda išvengti dviprasmybių ir suteikia būsimam kibernetinio saugumo pokyčių agentui reikiamą oficialų statusą bei autoritetą veikti.

Tik atlikus šiuos tris žingsnius, organizacija yra pasirengusi parinkti ir paskirti tinkamiausią kandidatą. Tolesniame skyriuje pateikiamas kontrolinis sąrašas, padėsiantis sėkmingai įgyvendinti šį vaidmenį.

1 pav. Vizualinės kibernetinio saugumo pokyčių agento vaidmens įgyvendinimo gairės (veiksmų planas)



7. KONTROLINIS SĄRAŠAS

Šioje dalyje pateiktas kontrolinis sąrašas yra skirtas patikrinti, ar įmonėje yra sudarytos visos pagrindinės sąlygos, būtinos sėkmingam kibernetinio saugumo pokyčių agento vaidmens įgyvendinimui. Šis sąrašas yra sudarytas remiantis bandomojo projekto „CyberAgent“ metu sukaupta patirtimi ir įžvalgomis.

7.1. VADOVŲ LYGMUO

[ ] Dėl pokyčių agento vaidmens įvedimo yra oficialiai susitarta ir jam numatytas reikiamas finansavimas (biudžetas).

[ ] Suteikti aiškūs įgaliojimai: apibrėžta veiklos apimtis, šiai funkcijai skiriamas laikas ir pavaldumo struktūra.

[ ] Apie darbuotojo paskyrimą į šias pareigas yra informuota visa organizacija.

[ ] Šio vaidmens ir jo efektyvumo peržiūra yra suplanuota per artimiausius 12 mėnesių.

[ ] Pokyčių agento darbo grafike yra rezervuotas laikas, skirtas tik šioms pareigoms vykdyti.

7.2. ŽMOGIŠKIEJI IŠTEKLIAI

[ ] Atrankos procesas buvo atviras visiems darbuotojams, nepriklausomai nuo jų lyties, išsilavinimo ar profesinės patirties.

[ ] Pristatant šį vaidmenį, pagrindinis dėmesys buvo skiriamas jo įtakai organizacijai, o ne techninėms žinioms.

[ ] Pokyčių agento atsakomybės yra oficialiai įtrauktos į jo pareigybės aprašymą arba metinius veiklos tikslus.

[ ] Nauji darbuotojai su kibernetinio saugumo pokyčių agentu yra supažindinami pirmųjų dienų adaptacijos (angl. onboarding) metu.

[ ] Yra kaupiami ir saugomi visi duomenys apie pokyčių agento išklausytus mokymus bei įgytus sertifikatus.

7.3. KIBERNETINIO SAUGUMO POKYČIŲ AGENTAS

[ ] Užsiregistruota „CyberAgent“ platformoje ir suderintas individualus mokymosi planas (programa).

[ ] Išklausytas bent vienas modulis ir gautas tai patvirtinantis sertifikatas.

[ ] Kolegos žino, kaip ir kokiais kanalais prireikus susisiekti su pokyčių agentu.

[ ] Užtikrintas reguliarus darbuotojų informavimas bei sąmoningumo ugdymas (rengiami susirinkimai, siunčiami pranešimai ar priminimai).

[ ] Yra nustatyta aiški tvarka, leidžianti darbuotojams patogiai pranešti apie įtartinas situacijas.

[ ] Grįžtamasis ryšys apie kibernetinio saugumo problemas bei klausimus yra reguliariai renkamas ir perduodamas (eskaluojamas) vadovams.

8. KAIP ĮVERTINTI ĮGYVENDINIMO SĖKMĘ

Kibernetinio saugumo pokyčių agento vaidmens įgyvendinimas reikalauja nuolatinio įsipareigojimo. Toliau pateikti rodikliai gali padėti MVĮ įvertinti, ar šis vaidmuo ilgainiui daro realią įtaką organizacijai.

[ ] Nuo pokyčių agento paskyrimo išaugo kibernetinio saugumo sąmoningumo didinimo veiklose dalyvaujančių darbuotojų skaičius.

[ ] Kibernetinio saugumo temos yra reguliariai aptariamos komandos susirinkimuose ir nebėra laikomi išskirtiniu ar neįprastu klausimu.

[ ] Darbuotojai žino, kas yra pokyčių agentas, ir drąsiai kreipiasi į jį, turėdami klausimų ar pastebėję problemų.

[ ] Padidėjo pranešimų apie įtartinus el. laiškus, incidentus ar galimas saugumo problemas skaičius (tai rodo didesnį darbuotojų budrumą).

[ ] Nuo pradinio paskyrimo pokyčių agentas baigė papildomus mokymo modulius.

[ ] Darbuotojų atsiliepimai apie kibernetinį saugumą įmonėje yra renkami periodiškai ir naudojami priimant tolesnius sprendimus.

8.1. METODINĖS GAIRĖS VADOVYBEI DĖL ŠABLONŲ ADAPTAVIMO IR INDIVIDUALIZAVIMO

Siekiant užtikrinti, kad kibernetinio saugumo pokyčių agento kvalifikacijos kėlimas virstų ilgalaikiu įmonės atsparumu grėsmėms, būtina vykdyti nuolatinę struktūruotą stebėseną. 3 lentelėje pateikiamas praktiškas veiklos sekimo šablonas, skirtas MVĮ vadovams įvertinti pradinį organizacijos lygį prieš mokymus bei išmatuoti realią saugumo kultūros pažangą, praėjus 6 ir 12 mėnesių po darbuotojo paskyrimo.

Vadovams šį šabloną rekomenduojama vertinti kaip lanksčias gaires. Atsižvelgiant į įmonės dydį, veiklos sektorių ir esamą infrastruktūrą, šią vertinimo matricą tikslinga pritaikyti ir išplėsti pagal individualius organizacijos poreikius:

- **Vertinimo skalių pritaikymas**
  Labai mažos įmonės (mikroįmonės, turinčios iki 10 darbuotojų) procentinius rodiklius gali supaprastinti iki tikslaus darbuotojų skaičiaus – taip bus lengviau stebėti ir fiksuoti duomenis.
- **Rodiklių išplėtimas**
  Labai skaitmenizuotose arba didelės rizikos aplinkose veikiančioms įmonėms rekomenduojama įtraukti papildomas specifines eilutes, pavyzdžiui: „% darbuotojų, naudojančių daugiafaktorį autentifikavimą (MFA)“ arba „Vidutinis reakcijos laikas į imituojamą grėsmę“.

- **Lokalizavimas**
  Stulpelį „Rekomenduojamas duomenų šaltinis“ svarbu suderinti su įmonėje faktiškai naudojamais vidinės komunikacijos kanalais (pavyzdžiui, duomenis rinkite per „Slack“, „MS Teams“ apklausas arba pildykite fizinius žurnalus trumpų komandos pasitarimų metu).

3 lentelė. Veiklos stebėsenos po paskyrimo šablonas MVĮ vadovams

Sėkmės rodiklis	**Vienetas / vertinimo skalė**	**Pradinis lygis (prieš mokymus)**	**Pažanga (po 6 mėnesių)**	**Tikslas (po 12 mėnesių)**	**Rekomenduojamas duomenų šaltinis**
Darbuotojų pasirengimas atpažinti sukčiavimą	% darbuotojų, gebančių tinkamai elgtis su įtartinais el. laiškais	%	%	%	Vidinė trumpoji apklausa (angl. pulse survey) arba platformos „CyberAgent“ duomenys
Temos integravimas į susirinkimus	Komandos susirinkimų, kuriuose buvo aptartas kibernetinis saugumas, skaičius	Skaičius	Skaičius	Skaičius	Komandos susirinkimų protokolai / darbotvarkės
Pranešimų apie incidentus aktyvumo rodiklis	Užregistruotų ir praneštų įtartinų incidentų skaičius	Skaičius/ mėn.	Skaičius/ mėn.	Skaičius/ mėn.	Vidinis saugumo incidentų žurnalas arba IT skyriaus grįžtamasis ryšys
Pokyčių agento žinomumas	% darbuotojų, tiksliai žinančių, kas yra pokyčių agentas	%	%	%	Trumpa vidinė apklausa (anketa)
Aktyvumas e. mokymosi platformoje	Darbuotojų, aktyviai dalyvaujančių mikromokymosi veiklose, skaičius	Skaičius	Skaičius	Skaičius	Platformos „CyberAgent“ vadovo analitinių duomenų skydelis (angl. dashboard)

IŠVADOS

Kibernetinis saugumas jau seniai nebėra tik didžiųjų organizacijų, turinčių atskirus IT skyrius, rūpestis. Nuolat kintant kibernetinių grėsmių aplinkai ir augant teisiniams bei reguliaciniams reikalavimams mažoms ir vidutinėms įmonėms (MVĮ) kyla pagrindinis klausimas – kaip jos gali apsisaugoti, naudodamos tik tuos išteklius, kuriuos realiai turi?

Kibernetinio saugumo pokyčių agento vaidmuo suteikia praktišką ir praktiškai pritaikomą atsakymą į šį klausimą. Tam nereikia samdyti naujų specialistų, investuoti į brangias priemones ar iš esmės pertvarkyti jau veikiančių procesų. Svarbiausia – organizacijoje atrasti tinkamą darbuotoją, suteikti jam reikiamų žinių bei įgaliojimus veikti ir sudaryti sąlygas, kad kibernetinio saugumo sąmoningumas taptų natūralia kasdienio darbo dalimi.

Projektas „CyberAgent“ ir vykdyti pilotiniai mokymai įrodė, kad tai yra įmanoma. Aštuoniose Europos šalyse MVĮ darbuotojai, neturintys techninio išsilavinimo ar patirties, sėkmingai baigė mokymus, prisiėmė šias pareigas ir pradėjo iš esmės keisti savo organizacijų požiūrį į kibernetinį saugumą. Rezultatai akivaizdūs: kai atsisakoma perteklinių pradinių reikalavimų, kai vaidmuo grindžiamas organizacine kultūra, o ne techninėmis žiniomis, ir kai įtrauktis tampa pamatiniu principu, o ne šalutiniu klausimu – pasiekiamas ilgalaikis pokytis.

Šis dokumentas – tai kvietimas žengti pirmąjį žingsnį. Veiksmų planas jau paruoštas, o reikalingi įrankiai – ranka pasiekiami. Šią funkciją gali sėkmingai įsidiegti bet kuri MVĮ, pasirengusi investuoti į savo darbuotojus.

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