UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RAPORT DE REZULTATE EVENIMENT

Raport de rezultate generate în urma evenimentului nr. 11

Up-grade: Cum îmi mențin securitatea informațiilor în mediul digital?

Fondul Social European

Programul Operațional Capital Uman 2014-2020

Axa prioritară 6 - *Educație și competențe*

Obiectiv tematic 10: *Efectuarea de investiții în domeniul educației, al formării și al formării profesionale în vederea dobândirii de competențe și a învățării pe tot parcursul vieții*

Prioritatea de investiții 10.iv: *Sporirea relevanței pe piața forțelor de muncă a educației și a sistemelor de formare, facilitarea tranziției de la educație la piața forțelor de muncă și consolidarea formării și a sistemelor de formare profesională, precum și a calității lor, inclusiv prin mecanisme de anticipare a competențelor, adaptarea programelor de învățământ și instituirea și dezvoltarea unor sisteme de învățare la locul de muncă, inclusiv a unor sisteme de învățare dual și programe de ucenicie*

Obiectiv specific 6.13: *Creșterea numărului absolvenților de învățământ terțiar universitar și non-universitar care își găsesc un loc de muncă urmare a accesului la activități de învățare/ cercetare/ inovare la un potențial loc de muncă, cu accent pe sectoarele economice cu potențial competitiv identificate conform SNC și domeniile de specializare inteligentă conform SNCDI*

Apel de proiecte: *POCU/626/6/13 Stagii de practică pentru studenți*

Titlul proiectului: ***INSPIRE - Inițiative Necesare de Stagii de Practică Inovative pentru Revitalizare Economică***

Contract POCU/626/6/13/133017, 11759/13.10.2020, **ID MySMIS: 133017**

INSPIRE

INSPIRE - Inițiative Necesare de Stagii de Practică Inovative pentru Revitalizare Economică

CUPRINS

1. CONTEXT

Evenimentul nr. 11: *„Up-grade: Cum îmi mențin securitatea informațiilor în mediul digital?”* din cadrul Think-Tank-ului INSPIRE a propus extinderea orizontului de cunoștințe practice ale studenților în domeniul digital, utilizării instrumentelor digitale/ TIC și în domeniul securității cibernetice sau în mediul online. Formatul de tip trei speakeri invitați a fost optim pentru evaluarea și discutarea problemelor specifice cu care se pot confrunta studenții în contextul unei amenințări cibernetice. Menținerea securității informaționale în mediul digital prezintă diverse sub-straturi și componente ce au fost detaliate în mod specific de fiecare speaker invitat. Evenimentul nr. 11 de Think-Tank debutează cu intervenția lui Rareș Popa, IT & Security specialist la Ausy Technologies Romania, care inițiază discuția cu aspecte generale privind utilizarea și securizarea terminalelor digitale, concentrându-se pe aspecte ce pot fi aplicate cu ușurință de majoritatea studenților în vederea asigurării unui nivel ridicat de securitate a informațiilor lor atunci când utilizează medii digitale sau online. Invitata Cristiana Deca, Managing Partner la Decalex, a abordat subiecte specifice despre păstrarea confidențialității datelor și informațiilor personale în mediul online, promovând importanța legislației GDPR. În final, Dumitra Dragoș, Threat Hunter la CrowdStrike Romania, a discutat cu studenții noțiuni avansate privind riscurile asociate atacurilor cibernetice și metode de menținere a securității informațiilor în mediul digital, oferind insight-uri cuprinzătoare în baza experienței profesionale proprii. Activitatea suport de Think-Tank se bazează pe interacțiunea cuprinzătoare dintre studenți-profesori-angajatori pentru a dezvolta noi teme de discuție și pentru a implementa activități îmbunătățite în cadrul proiectului INSPIRE – *Inițiative Necesare de Stagii de Practică Inovative pentru Revitalizare Economică* sau în afara acestuia de către terțe părți care ar putea implementa coerent sau ar putea utiliza ideile dezvoltate pentru a îmbunătăți semnificativ situația cu privire la problemele identificate.

2. OBIECTIVE

Obiectivele evenimentului nr. 11 *„Up-grade: Cum îmi mențin securitatea informațiilor în mediul digital?”* au vizat diseminarea instrumentelor practice prin care studenții pot asigura un nivel ridicat de securitate în mediul digital al informațiilor lor. În plus, evenimentul a urmărit diseminarea de metode practice prin care studenții pot identifica și reacționa la vulnerabilitățile securității informaționale în medii digitale. Evenimentul a vizat fundamentarea cunoștințelor diseminate prin intermediul

sesiunilor speciale de întrebări și răspunsuri în care studenții puteau interacționa în mod direct cu speakerii invitați. În plus, evenimentul a vizat conectarea studenților cu potențiali angajatori ce au expus diferite oportunități redate de domeniul IT&C sau de domeniul securității cibernetice ce pot fi accesate de studenți.

3. REZULTATE

Evenimentul de tip Think-Tank nr. 11 „*Up-grade: Cum îmi mențin securitatea informațiilor în mediul digital?*" a fost împărțit în trei intervenții, Rareș Popa-Cristiana Deca-Dumitra Dragoș între care au fost intercalate sesiuni de întrebări și răspunsuri în vederea oferirii studenților posibilității de a adresa întrebări în retrospectivă despre informațiile comunicate anterior, sau despre alte subiecte relevante pentru studenți din perspectiva asigurării securității în mediul digital.
În cadrul evenimentului au fost abordate subiecte diferite ce au vizat diseminarea într-un mod eficient a informațiilor, metodelor și instrumentelor legate asigurarea unui nivel ridicat de siguranță informațională în mediile digitale sau online, vizând următoarele întrebări:

Cum ne putem da seama că avem un virus care ne copiază, fără să știm, datele din calculator?
Pentru asigurarea mediilor sau terminalelor digitale împotriva amenințărilor de tip virus sau malware care copiază în background datele din calculator s-a recomandat utilizarea sistemelor de tip antivirus actualizate recurent ce vizează scanarea în timp real a disfuncționalităților. Acest lucru va asigura că potențiali atacatori nu vor putea exploata vulnerabilitățile terminalului și nu vor permite acestora preluarea, executarea și rularea de programe malițioase la nivelul terminalului de lucru. Se aduce în discuție faptul că variantele gratuite a soluțiilor antivirus disponibile pe internet nu oferă o protecție completă împotriva atacurilor, fiind recomandate variantele care încorporează module adiționale de detectarea și combatere a amenințărilor de tip spyware sau malware.

În cazul stocării de tip Cloud, dintr-un fișier virusat se pot transmite viruși în toate celelalte fișiere încărcate?
Fișiere stocate în Cloud (cu extensii comune precum PDF, Excel, Word etc.) sunt fișiere stocate pe servere fizice conectate la internet pentru care terminalele conectate au drepturi de admin (drepturi nelimitate privind descărcarea, modificarea, actualizarea etc.), astfel eventuale programe de tip malware sau virus pot utiliza aceste vulnerabilități pentru injectarea de viruși și modificarea, criptarea sau ștergerea fișierelor.

De ce nu ar trebui folosit file sharing-ul?

File sharing-ul este o practică riscantă din punct de vedere al securității digitala, mai ales la nivel de companie unde virușii pot cripta și interzice accesul la fișierele partajate între membrii echipei de lucru. Totuși, în contexte specifice sau limitate file sharing-ul poate fi utilizate, dar se recomandă în continuare ca acest mod de lucru să fie utilizat în cazul conexiunilor la rețele sigure și criptate.

În continuarea evenimentului, intervenția Cristianei Deca s-a concentrat pe alte aspecte legate de cybersecuritate, însă a vizat și discutarea aspectelor asociate menținerii confidențialității informațiilor în mediul online, vizând creșterea conștientizării cu privire la drepturile existente prin intermediul legislației GDPR. Atât cybersecuritate și siguranța confidențialității par să fie aspecte trecute cu vederea de către studenți și chiar profesioniști din domenii diverse, dar care sunt esențiale pentru orice utilizator din mediul digital sau cel online.

Care sunt cele mai mari riscuri în materie de atacuri cibernetice, și ce măsuri de urgență sau de siguranță am putea lua?

Atacurile cibernetice la nivel de business sunt văzute cu claritate, întrucât majoritatea companiilor au sau sunt obligate prin natura activității să aibă echipe specializate de a răspunde incidentelor ce amenință securitatea digitală a informațiilor. Această echipă include de cele mai multe ori cel puțin un manager IT, expert în protecția datelor cu caracter personal și o persoană din management. Această echipă trebuie să identifice tipul de atac, să încerce să minimizeze extinderea acestuia, și în final să analizeze care sunt daunele provocate de atac. Pentru diminuarea extinderii unui atac se recomandă deconectarea de la rețea (sau specific de la rețeaua afectată), deconectarea tuturor tipurilor de terminale ce au acces remote și schimbarea tuturor parolelor. Cele mai comune tipuri de atacuri sunt cele tip spam care pot extrage informații financiare, medicale etc. care pot avea repercusiuni grave asupra persoanelor afectate. Dacă acest tip de scurgeri informaționale se întâmplă la nivel de companie unde sunt afectați clienții sau angajații, compania poate raporta incidentul autorităților în maxim 72 de ore de la incidența acestuia.

Care sunt cele mai utile metode concrete pentru a ne crește securitatea informațiilor digitale?

Este recomandată reducerea utilizării motorului de căutare Google și înlocuirea acestuia cu DuckDuckGo. Alte soluții sau instrumente recomandate sunt: utilizarea Brave ca browser implicit, utilizarea AdBlockerelor (instrumente de blocare a reclamelor în mediul online), utilizarea ProtonMail ca provider/ serviciu de email care filtrează și blochează mesajele tip spam, menținerea actualizărilor de software, utilizarea de parole diferențiate și generate cu un grad de protecție îmbunătățit, transmiterea criptată sau arhivată a atașamentelor transmise prin email.

Dacă pe platforma proprie, clienții mei solicită să își păstreze anonimatul, cum le pot respecta această decizie, dar în același timp să îmi păstrez platforma sigură?

Păstrarea anonimității informațiilor utilizatorilor poate fi posibilă în funcție de obiectul platformei. În cazul platformelor generale de informare a utilizatorilor, confidențialitate acestora trebuie și poate fi păstrată. Totuși, în cazul platformelor din domeniul financiar sau medical confidențialitatea utilizatorilor nu poate fi menținută pentru că este necesară prelucrarea datelor în vederea colaborării cu utilizatorul, prestării serviciilor sau livrării de produse.

În final, Dumitra Dragoș atenționează asupra multitudinii de situații prin care utilizatorii sau companiile pot fi expuși atacurilor cibernetice, dar indică anumite soluții de protecție împotriva acestora deoarece, chiar și în fază incipientă, un atac cibernetic poate conduce la pierderea ireversibilă a unor date sau informații importante.

Care sunt cele mai comune tipuri de atacuri cibernetice?

Tipurile de atacatori pot fi clasificați în funcție de următoarele criterii: atacatorii care vizează producerea de foloase financiare direct sau indirect, cel mai frecvent fiind caracterizați de atacuri care criptează fișierele sau datele și cer bani pentru decriptarea acestora; atacatorii care vizează metode de extorcare sau șantajare care fură și replică informații, inclusiv website-urile guvernamentale sau corporative.

Sistemul de operare Mac OS/IOS este mai sigur decat Windows?

Se atenționează asupra faptului că nu există sisteme de operare mai sigure decât altele, ponderea atacurilor cibernetice fiind relativ egal distribuite pentru toate sisteme de operare populare: MacOS, Windows sau Linux. În general, există un număr mai mare de atacuri cibernetice asupra sistemelor de operare Windows pentru că sunt mai populare în rândul utilizatorilor, dar pentru fiecare tip de sistem de operare se recomandă o soluție antivirus actualizată și capabilă să detecteze problemele de vulnerabilitate. Se atenționează asupra faptului că nu toate soluțiile de tip antivirus pot detecta în întregime vulnerabilitățile sistemului, deci trebuie selectat un antivirus oferit de un provider sigur ce cuprinde instrumente diverse.

4. Concluzii și Propuneri

În urma discuției evenimentului nr. 11 „*Up-grade: Cum îmi mențin securitatea informațiilor în mediul digital?*” pot fi identificate anumite arii de intervenție pentru care se pot dezvolta acțiuni concrete prin care se pot actualiza competențele specifice ale studenților cu privire la asigurarea securității digitale a informațiilor lor în vederea îmbunătățirii stilului de viață online, a

comportamentului în mediul digital și a competențelor digitale ce pot fi utilizate în mediul profesional de către studenți:

Cursuri TIC la nivel universitar

Formarea studenților la nivel universitar în centre digitale/ tehnologice în domeniul utilizării mijloacelor informatice sau TIC, atât pentru operațiuni de bază, dar și pentru noțiuni avansate legate de rezolvarea de probleme, crearea de conținut digital și asigurarea securității informațiilor în mediul digital.

Cursuri TIC la nivel de companie angajatoare

Asumarea unor ținte anuale de către angajatori privind formarea angajaților pentru operarea terminalelor informatice sau alte operațiuni TIC, vizând noțiuni de bază și avansate.

Actualizarea cerințelor profesionale de angajare

Actualizarea cerințelor la angajare privind competențele digitale, impulsionând mediul educațional și piața de muncă să vizeze pregătirea specifică în domenii asociate competențelor digitale sau tehnologice.

Responsabil facilitare cooperare și dialog stakeholderi 4

Rusu Gabriela