Co-funded by the Erasmus+ Programme of the European Union

InCyT træningsmoduler

Informationssikkerhed for ledere **Enhed 1 uge 1** **Enhedens navn: Introduktionswebinar**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑**Andet**
Læringsansvarlig	• Gabriel Vladut • Valentin Istratie
Læringsaktivitetsmål	1. Om Erasmus+ InCyT- projektet 2. Mål 3. Resultater og produkter 4. Sådan beskytter du dig selv mod cyberangreb 5. Træning og vejledning 6. Social ingeniørkunst 7. Socialt netværk (sociale medier)
Færdigheder, der skal opnås	• TS3 netværkssikkerhed • TS4 Penetration (udnyttelige sårbarheder) test • SS3 Kognitiv og adfærdsanalyse
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?***
	• For at lære om Erasmus+ InCyT-projekt/målsætninger/resultater og produkter • Sådan beskytter du dig selv mod cyberangreb • Træning og vejledning • Social engineering/socialt netværk (sociale medier)

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.

Co-funded by the Erasmus+ Programme of the European Union

Kort information om modulet

Beskrivelse
InCyT er et Erasmus+-projekt, der har til formål at skabe en ramme, en metodologi for uddannelse, som giver en mekanisme for erhvervsuddannelse og virksomheder til at beskrive de kompetencer og færdigheder, der er nødvendige i cybersikkerhed for fagfolk og ikke professionelle for at undgå cyberangreb, samt digitale huller og andre. NIST's National Initiative for Cyber Security Education (NICE) understreger, at det bør gøres et afgørende skridt i retning af at afhjælpe mangel på "mennesker med viden, færdigheder og evner til at udføre de opgaver, der kræves til cybersikkerhedsarbejde." En sådan arbejdsstyrke vil omfatte "tekniske og ikke-tekniske roller, der er bemandet med kyndige og erfarne mennesker." Projektet vil gerne implementere nogle løsninger i denne sammenhæng. Formålet er først og fremmest at udvikle en ramme, som giver EUD og virksomheder en mekanisme til at beskrive de digitale huller og andre nødvendige i cybersikkerhed for fagfolk og ikke fagfolk for at undgå cyberangreb og hjælpe dem med at forbedre denne situation. Under hensyntagen til fordelene ved tværfaglige trænings- og mentorprogrammer, især inden for cybersikkerhed, vil projektet udvikle og teste digitale tværfaglige træningsprogrammer understøttet af e-mentoring for SMV'er og tilpasse det til EUD. Samarbejde og kommunikation mellem undervisere, forskere og mennesker, der bruger informationsteknologier, er nødvendigt. Et problem er, at virksomheder, især SMV'er med færre ressourcer, har brug for hjælp til at værdsætte deres medarbejderes kompetencer og kompetencegab, metoder til at evaluere den eksisterende situation samt bruge uddannelsesmuligheder til at omskolde deres medarbejdere. Eleverne kunne blive informeret om sådanne aspekter ved at læse den tilsvarende tekst, se streaming webinarer og løse øvelser i eget tempo. Alle disse dokumenter er på den digitale interaktive projektplatform. Eleverne kan teste deres svar på selvevalueringsøvelser. Svarene på andre øvelser skal gemmes på det tilsvarende diskussionsforum og diskuteres med mentoren på det fælles tilrettelagte møde en gang om ugen. Eleven kan arbejde sammen med andre og vejlede især under møderne. De vil blive støttet til at udvikle e-portfolio, der er vigtig for refleksion og evaluering af træningen.

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.

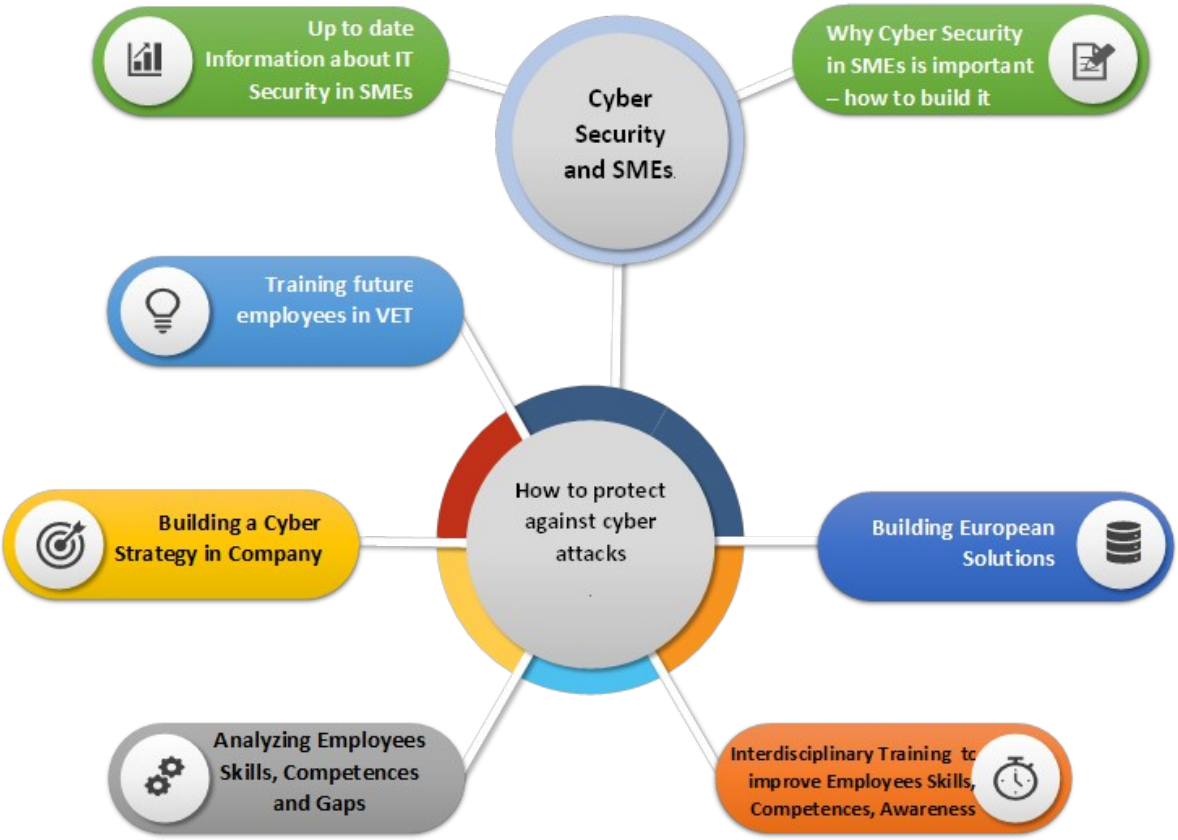
Co-funded by the Erasmus+ Programme of the European Union

Lærematerialets indhold

Kompetenceramme

Der vil være 3 transnationale møder i vores projekt. Det var planlagt i 3., 13. og 20. måned af projektet. Der vil blive afholdt nogle ekstra projektmøder, da vi mener at 3 møder ikke vil være nok til at køre et 24 måneders projekt. Disse møder er online og afholdes regelmæssigt hver måned. Projektledelsen vil organisere disse projekter.

Projekterne vil blive ledet af projektkoordinatoren, WP-lederen. Der vil være 7 multiplikatorbegivenheder i vores projekt. Hver partnerinstitution vil organisere disse aktiviteter for at popularisere projektideen i sit eget land og for at dele de udviklede produkter. Hver partnerinstitution vil afholde den tværfaglige uddannelse for SMV-ansatte og -lærere i Cybersikkerhedsaktivitet i deres eget land.



Figur 1: Aktiviteter støttet af InCyT- projektet

Mål

InCyT - projektet vil gerne implementere nogle løsninger:

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.

Co-funded by the Erasmus+ Programme of the European Union

- Udviklingen af et rammeværk, som giver EUD og virksomheder en mekanisme til at beskrive de kompetencer og færdigheder, der er nødvendige inden for cybersikkerhed for fagfolk og ikke professionelle for at undgå cyberangreb samt digitale huller og andre.
- Under hensyntagen til fordelene ved tværfaglige trænings- og mentorprogrammer, især inden for cybersikkerhed, vil projektet udvikle og teste digitale tværfaglige uddannelsesprogrammer, der understøttes og en samarbejdsplatform for e-læring for SMV'er
- Tilpas det til EUD.
- Udvikle en europæisk overførselsmodel
- Under hensyntagen til fordelene ved tværfaglige trænings- og mentorprogrammer, især inden for cybersikkerhed, vil projektet udvikle og teste digitale tværfaglige træningsprogrammer understøttet af e-mentoring for SMV'er og tilpasse det til EUD.

Projektets resultater vil være:

- Metodisk ramme for implementering
- Eksisterende og fulgte uddannelser (kurser)
- Muligheder for forbedringer af disse ved brug af tværfaglighed og mentorordninger.
- Lærings- og mentormetode

Produkter :

1. Ramme

2. Et digitalt tværfagligt cybersikkerhedsundervisningsmateriale for SMV'er understøttet af mentorordninger og en tilpasset metodik til et specialuddannelsesforløb.

3. En digital platform til at understøtte uddannelsen

4. Rapportér, hvordan tværfaglige kompetencer giver fordele for SMV og moms.

5. Europæisk overførselsmodel for den testede tværfaglige træning og mentorordninger

Partnere fra: Tyskland (koordinator), Tyrkiet, Polen, Italien, Østrig, Danmark, Rumænien.

Aktiviteter

- Metodologisk ramme for cybersikkerhed - førende organisationer : IAT, Tyskland, Italien
- Et digitalt tværfagligt træningsmateriale for cybersikkerhed - førende organisation : St. Pölten University of Applied Sciences, Østrig
- IKT-platform for cybersikkerhed - førende organisation : IPA, Rumænien

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.

Co-funded by the Erasmus+ Programme of the European Union

- Metodisk model for cybersikkerhed - førende organisation : Politechnik University, Polen
- Overførbarhedsmodel - førende organisation : European Training Center København, Danmark
- Multiplikatorbegivenheder - førende organisation : Tyrkiet

Sådan beskytter du dig selv mod cyberangreb

Den digitale økonomi er primært baseret på data. I æraen med Industri 4.0, cyberfysiske systemer og tingenes internet bliver flere og flere produkter og processer digitaliseret. Cybersikkerhed, hvilket betyder beskyttelse af disse data og tilhørende informationsbehandlingssystemer, er mere relevant i dag end på noget tidspunkt i den økonomiske historie.

Forretningsprocesser kan være væsentligt forstyrret, bremset eller endda fuldstændig blokeret, for eksempel hvis dataregistreringer er forkerte, ufuldstændige eller slet ikke tilgængelige, datasynkronisering mellem systemer er forstyrret, it-systemer fungerer forkert eller fejler fuldstændigt.

Især SMV'er er mål for kriminel aktivitet relateret til disse spørgsmål. I modsætning til store virksomheder er deres ressourcer begrænsede - og hackere ved det! SMV'er er rygraden i økonomien i Europa, hvilket betyder, at over 99% af virksomhederne i Tyskland er SMV'er.

Mere end halvdelen af arbejdsstyrken er ansat i SMV'er. Det er derfor nødvendigt at hjælpe SMV'er med at undgå cyberangreb .

Cyber Security Education Initiative påpeger, at der bør tages et kritisk skridt for at imødegå manglen på "individer med viden, færdigheder og evner til at udføre de opgaver, der kræves til cybersikkerhedsarbejde."

En sådan gruppe omfatter "tekniske og ikke-tekniske funktioner, der besættes af medarbejdere med viden og erfaring."

Det er dog svært at skabe en arbejdsstyrke med de nødvendige tværfaglige kompetencer og at løse problemet med kommunikation mellem undervisere, forskere og folk, der bruger informationsteknologi.

Samarbejde og kommunikation mellem disse grupper er nødvendigt.

Et problem er, at virksomheder, især SMV'er med færre ressourcer, har brug for hjælp til at vurdere deres medarbejderes kompetencer og huller ved at bruge digitale metoder til at forbedre den eksisterende situation og tilrettelægge uddannelsesmuligheder for at omskole deres medarbejdere.

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.

Co-funded by the Erasmus+ Programme of the European Union

Træning og vejledning

Iværksættere, herunder fremtidige, har brug for komplekse måder at tænke på og evnen til at forstå og integrere viden fra forskellige sektorer, hvilket kræver tværfaglig læring.

Komplekse tekniske problemer kræver at skabe en tværfaglig situation på en næsten naturlig måde.

I en tværfaglig tilgang bør eleverne integrere information fra forskellige discipliner og områder.

De udvikler en tværfaglig forståelse, lærer at integrere ekspertiseområder og disciplinspecifikke måder at tænke på.

Dette øger kognitive færdigheder og kritisk tænkning mere end gennem enkelt disciplinære midler.

Social ingeniørkunst

- det betyder at manipulere mennesker (ofte ved hjælp af psykologiske metoder) for at få adgang til data, dokumenter og information af interesse for angriberen.
- er en af de vigtigste trusler mod informationssikkerheden i dag og er en effektiv form for cyberkriminalitet.
- kunne have farlige konsekvenser, for eksempel databrud, mere end nogen anden form for angreb.
- angrebene har et økonomisk formål, og dermed har organisationer tabt betydelige pengebeløb.
- det er særligt farligt, fordi det er mere afhængigt af menneskelige fejl end på sårbarheder i software og operativsystemer.

Virksomhederne :

- de kunne lide tabt produktivitet, et fald i medarbejdernes moral og vanskeligheder med at komme sig.
- de har skade på omdømmet, fordi kunderne ikke er overbeviste om, at organisationen kan beskytte sig selv.
- ofte nødt til at udløse en gammel hændelsesreaktion.
- skal levere sikkerhedssoftware til at forhindre fremtidige angreb.
- de ville ofte skulle omskole medarbejdere for at være klar til angreb.

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.

Co-funded by the Erasmus+ Programme of the European Union

Social ingeniøruddannelse (cyberbevidsthed)

- af medarbejdere og ledere, for hvem det er vigtigt at anerkende socialtekniske angreb, fordi risikoen for at blive offer er høj.
- kunne inkluderes i fællesskabs-, individ- og borgersikkerhedsbevidsthedsprogrammer og beskytte enkeltpersoner og deres organisation.
- er især mangelfuld i SMV'er, der har færre ressourcer, så de bør hjælpes til at tage cyberbevidsthedstræning seriøst og give medarbejderne mulighed for at tage den.

Social Engineering Attack Lifecycle

Angriber:

- efterforsk først det målrettede offer for at indsamle de nødvendige grundlæggende oplysninger, såsom indgangspunkter og svage sikkerhedsprotokoller, der er nødvendige for angrebet.
- prøv derefter, vind ofrets tillid og giv incitamenter til handlinger, der normalt ikke er sikkerhedspraksis, såsom at blive følsomme oplysninger eller give adgang til kritiske ressourcer.

Figur 2 forklarer livscyklussen for et angreb.

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.

Co-funded by the Erasmus+ Programme of the European Union

Figur 2: Livscyklus for et angreb

Socialt netværk

- er blevet meget populær i de senere år, og giver brugerne en platform til at kommunikere med deres familie, venner og kolleger.
- og Social Networking henviser til brugen af internetbaserede sociale netværkssider til at forbinde og kommunikere med venner, familie, kolleger, klienter eller kunder.
- de har deres servere i datacentre, der er placeret sammen med de vigtigste netværksadgangspunkter på internettet.

Sociale medier roller (figur 3) viser nogle områder, hvor sociale medier spiller en rolle:

- Underholdning
- opbygning af forretningsmuligheder
- at gøre karriere
- at forbedre sociale færdigheder
- at udvikle relationer til andre individer

Figur 3: Roller i det sociale netværk

Socialt netværk :

- er et fundament for marketingfolk på udkig efter kunder for at øge brandgenkendelsen, fremme brandloyalitet, forbedre konverteringsraterne, give adgang og engagement med nye, nye og gamle kunder.
- gøre det muligt, ved at dele blogindlæg, billeder, videoer eller kommentarer på sociale netværk, for flere at besøge virksomhedens hjemmeside og blive kunder.
- det gør det svært at følge med ændringer og påvirker også en virksomheds succesrate for

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.

Co-funded by the Erasmus+ Programme of the European Union

markedsføring.

De mest populære sociale netværkssider (sociale medier) i USA og Europa er:

- Facebook
- Instagram
- Twitter
- Youtube
- WhatsApp
- LinkedIn, der hjælper med at forbinde professionelle med kolleger, forretningsforbindelser og arbejdsgivere.

Socialt netværk er baseret på at udvikle og vedligeholde personlige og forretningsmæssige relationer ved hjælp af teknologi og sociale netværkssider (Social Media), der giver folk og virksomheder mulighed for at forbinde med hinanden, udvikle relationer, dele information, ideer og budskaber.

Familiemedlemmer kunne holde forbindelsen via personlige sociale netværk som Facebook, dele billeder og sende andre beskeder om deres liv.

Folk kan også forbinde sig med andre (fremmede), der deler de samme interesser.

Der er også ulemper ved sociale medier, herunder spredning af misinformation og de høje omkostninger ved at bruge og vedligeholde profiler på sociale medier.

Funktionaliteten af sociale platforme kan klassificeres i:

Netværksfunktioner tjener til at fremme sociale relationer mellem brugere inden for virtuelle platforme og giver funktionalitet til at bygge og vedligeholde den sociale netværksgraf.

Datafunktioner er ansvarlige for at styre brugerleveret indhold og kommunikation mellem brugere, der hjælper med at forbedre (udvide) brugerinteraktion og gøre platformen mere attraktiv

Adgangskontrolfunktioner har til formål at implementere brugerdefinerede privatlivsforanstaltninger og begrænse uautoriseret adgang til brugerleveret data og information.

Fordele og ulemper ved sociale netværk

Fordele

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.

Co-funded by the Erasmus+ Programme of the European Union

- Sociale medier giver virksomheder mulighed for at:
- For at komme i kontakt med nye og eksisterende kunder.
- at kunne skabe, promovere og øge brand awareness.
- at stole på anmeldelser og kommentarer fra deres klientel er vigtige for at øge brandsalget og højere placeringer i søgemaskinerne.
- for at kunne etablere et nyt brand. at demonstrere et højt serviceniveau til sine kunder.
- at kunne forbedre produkter og relationer til forbrugerne.

Ulempe

- de kan bidrage til spredning af misinformation.
- kan have en negativ indflydelse på virksomheder, fordi kritik af et brand har spredt sig meget hurtigt på sociale medier.
- kræver arbejdstimer og omkostninger hver uge for at opbygge og vedligeholde en virksomhedsprofil.

Sikkerhed og privatliv i sociale netværk

- Information, der deles på sociale netværk og medier, spredes meget hurtigt, hvilket gør det attraktivt for angribere at få dem.
- Sikkerheds- og privatlivsproblemer relateret til brugerdelt information, når en bruger uploader personligt indhold såsom fotos, videoer og lyd, bør respekteres, fordi angriberen kan ondsindet bruge de delte oplysninger til illegitime formål.
- Manglende brugerbevidsthed om sikkerhed og privatliv har potentiale til at føre til forskellige cyberangreb gennem sociale medier.

Trusler kan opdeles i tre kategorier:

- Konventionelle trusler omfatter trusler, som brugere er stødt på siden begyndelsen af det sociale netværk.
- Moderne trusler er angreb, der bruger avancerede teknikker til at kompromittere brugerkonti.
- Målrettede angreb er angreb rettet mod en bestemt bruger, som kan begås af enhver bruger til forskellige personlige vendettaer.

Løsninger til sociale netværksoperatører

- Godkendelsesprocedurer såsom CAPTCHA, multifaktorautentificering og billedidentifikation af venner er blevet foreslået.
- Sikkerheds- og privatlivsindstilling for at give kunden mulighed for at indtaste personlige

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.

Co-funded by the Erasmus+ Programme of the European Union

oplysninger fra uønsket adgang fra udenforstående eller applikationer.

Brugerrapporter om enhver form for misbrug eller politikovertrædelser af enhver bruger på deres netværk. det vil sige, at når Facebook modtager en brugerrapport, bliver den gennemgået og fjernet i henhold til Facebooks community-standarder.

Spørgsmål :

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne

1. Hvad er dine forventninger til InCyT- projektet
2. Sådan beskytter du dig selv mod cyberangreb
3. Hvad er en social engineering
4. Socialt netværk (sociale medier)

Selvevalueringsspørgsmål. Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

- Sådan beskytter du dig selv mod cyberangreb
- Hvad er en social engineering
- Socialt netværk (sociale medier)

Vedhæftede filer

PowerPoint-præsentation
Video film

Referencer:

- InCyT – Tværfaglig cybertræning
- Gendannelse af cyberhændelser
- Minimer cyberangreb - cyberresiliensstrategi
- Sådan forhindrer du cyberangreb: Top måder at beskytte dig selv på
- Social Media Security: Hvor sikre er dine oplysninger?
- Intern kontrol over informationssystemer

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.

Co-funded by the Erasmus+ Programme of the European Union

- Adoption af sociale medier bringer nye risici
- Social Media Security – 5 sikkerhedstip
- 19 Bedste praksis for social mediesikkerhed

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.