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

Moduli di formazione InCyT

Sicurezza delle informazioni per manager **Unità 1 Settimana 1** **Nome dell'unità: Webinar introduttivo**	
Attività di apprendimento	❑ **Webinar**❑ **Esercitazioni**❑ **Workshop**❑ **Presentazione**❑ **Altro**
Apprendimento responsabile	• Gabriel Vladut • Valentin Istratie
Obiettivi dell'attività di apprendimento	1. Informazioni sul progetto Erasmus+ InCyT 2. Obiettivi 3. Risultati e prodotti 4. Come proteggersi dagli attacchi informatici 5. Formazione e tutoraggio 6. Ingegneria sociale 7. Rete sociale (Social Media)
Competenze da acquisire	• Sicurezza di rete TS3 • TS4 Test di penetrazione (vulnerabilità sfruttabili) • SS3 Analisi cognitiva e comportamentale
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?***
	• Per conoscere il progetto Erasmus+ InCyT / obiettivi / risultati e prodotti • Come proteggersi dagli attacchi informatici • Formazione e tutoraggio • Ingegneria sociale / Rete sociale (Social Media)

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

Informazioni sintetiche sul modulo

Descrizione
InCyT è un progetto Erasmus + che mira a creare un quadro, una metodologia per la formazione, che fornisca un meccanismo per l'istruzione e la formazione professionale e per le aziende per descrivere le competenze e le abilità necessarie in materia di sicurezza informatica per i professionisti e non, al fine di evitare attacchi informatici, nonché lacune digitali e altro. L'Iniziativa nazionale per l'educazione alla sicurezza informatica (NICE) del NIST sottolinea che si tratta di un passo fondamentale per rimediare alla carenza di "persone con le conoscenze, le competenze e le abilità necessarie per svolgere i compiti richiesti dal lavoro sulla sicurezza informatica". Tale forza lavoro comprenderà "ruoli tecnici e non tecnici con personale competente ed esperto". Il progetto intende implementare alcune soluzioni in questo contesto. L'obiettivo è innanzitutto lo sviluppo di un quadro di riferimento, che fornisca un meccanismo per l'istruzione e la formazione professionale e per le aziende per descrivere le lacune digitali e le altre necessarie per la sicurezza informatica di professionisti e non professionisti, al fine di evitare attacchi informatici e aiutarli a migliorare la situazione. Tenendo conto dei vantaggi dei programmi di formazione e tutoraggio interdisciplinari, in particolare nel campo della sicurezza informatica, il progetto svilupperà e testerà programmi di formazione digitale interdisciplinare supportati da e-mentoring per le PMI e li adatterà all'istruzione e alla formazione professionale. È necessaria la collaborazione e la comunicazione tra educatori, ricercatori e persone che utilizzano le tecnologie dell'informazione. Un problema è che le aziende, in particolare le PMI con minori risorse, hanno bisogno di aiuto per valutare le competenze e le lacune dei propri dipendenti, i metodi per valutare la situazione esistente e le possibilità di formazione per riqualificare i propri dipendenti. I discenti possono essere informati su questi aspetti leggendo il testo corrispondente, guardando i webinar in streaming e risolvendo gli esercizi al proprio ritmo. Tutti questi documenti sono presenti sulla piattaforma digitale interattiva del progetto. I discenti possono verificare le loro risposte negli esercizi di autovalutazione. Le risposte agli altri esercizi devono essere salvate sul forum di discussione corrispondente e discusse con il tutor durante l'incontro comune organizzato una volta alla settimana. Gli studenti possono lavorare in modo cooperativo con gli altri e con il tutor, in particolare durante gli incontri. Saranno aiutati a sviluppare un e-portfolio importante per la riflessione e la valutazione della formazione.

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

Contenuto del materiale didattico

Quadro delle competenze

Il nostro progetto prevede 3 incontri transnazionali. Sono stati programmati al 3°, al 13° e al 20° mese del progetto. Verranno organizzati altri incontri del progetto, poiché riteniamo che 3 incontri non siano sufficienti per gestire un progetto di 24 mesi. Questi incontri sono online e si tengono regolarmente ogni mese. Il team di gestione senior del progetto organizzerà questi progetti.

I progetti saranno guidati dal coordinatore del progetto, il leader del WP. Il nostro progetto prevede 7 eventi moltiplicatori. Ogni istituto partner organizzerà queste attività per divulgare l'idea del progetto nel proprio Paese e per condividere i prodotti sviluppati. Ciascuna istituzione partner gestirà la formazione interdisciplinare per dipendenti e insegnanti delle PMI in materia di sicurezza informatica nel proprio Paese.

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

Obiettivi

Il progetto InCyT realizzerà alcune soluzioni:

- Sviluppo di un quadro di riferimento che fornisca un meccanismo per l'istruzione e la formazione professionale e per le aziende per descrivere le competenze e le abilità richieste nel campo della sicurezza informatica per i professionisti e non per evitare gli attacchi informatici, nonché le lacune digitali e altro.
- Progetto e realizzazione di programmi di formazione digitale interdisciplinare e una piattaforma di e-learning collaborativa per le PMI, considerando i vantaggi dei programmi di formazione e tutoraggio interdisciplinari, soprattutto nel campo della sicurezza informatica.
- Sviluppo di un modello europeo di trasferibilità
- Sviluppo e realizzazione di programmi di formazione digitale interdisciplinare supportati da e-mentoring per le PMI e adattamento all'istruzione e alla formazione professionale.

I risultati del progetto saranno:

- Un quadro metodologico per l'attuazione.
- Formazione esistente e frequentata (corsi).
- Opportunità di migliorarli attraverso l'uso dell'interdisciplinarità e del tutoraggio.
- Metodologia di apprendimento e tutoraggio.

Prodotti:

1. Un quadro di riferimento
2. Materiale di formazione digitale interdisciplinare sulla sicurezza informatica per le PMI, supportato da un tutoraggio e da una metodologia adattata a un corso di formazione professionale.
3. Una piattaforma digitale a supporto della formazione
4. Individuazione di competenze interdisciplinari che forniscono vantaggi alle PMI.
5. Un modello europeo di trasferibilità della formazione interdisciplinare e il tutoraggio

Partner da: Germania (coordinatore), Turchia, Polonia, Italia, Austria, Danimarca, Romania.

Attività

- Quadro metodologico per la sicurezza informatica - Organizzazioni leader: IAT, Germania, Italia
- Produzione di materiale di formazione digitale interdisciplinare sulla sicurezza informatica - Organizzazione leader: Università di Scienze Applicate di St. Pölten, Austria
- Piattaforma ICT per la sicurezza informatica - Organizzazione leader: IPA, Romania
- Modello metodologico per la sicurezza informatica - Organizzazione leader: Università Politechnik, Polonia
- Modello di trasferibilità - Organizzazione leader: Centro Europeo di Formazione di Copenaghen, Danimarca
- Multiplier Events - Organizzazione leader: Turchia

Come proteggersi dagli attacchi informatici

L'economia digitale si basa principalmente sui dati. Nell'era dell'Industria 4.0, dei sistemi cyber-fisici e dell'Internet of things sempre più prodotti e processi sono digitalizzati. La cybersecurity, ovvero la protezione di questi dati e dei relativi sistemi di elaborazione delle informazioni, è più importante oggi che in qualsiasi altro momento della storia economica.

I processi aziendali possono essere significativamente interrotti, rallentati o addirittura bloccati, ad esempio se i record di dati sono errati, incompleti o non sono affatto disponibili, se la sincronizzazione dei dati tra i sistemi è interrotta, se i sistemi IT funzionano in modo errato o se falliscono completamente.

Le PMI, in particolare, sono bersaglio di attività criminali legate a questi problemi. A differenza delle grandi aziende, le loro risorse sono limitate e gli hacker lo sanno bene! Le PMI sono la spina dorsale dell'economia europea: oltre il 99% delle aziende in Germania sono PMI.

Più della metà della forza lavoro è impiegata nelle PMI. È quindi necessario aiutare le PMI a evitare gli attacchi informatici.

La Cyber Security Education Initiative sottolinea che è necessario compiere un passo fondamentale per affrontare la mancanza di "individui con le conoscenze, le competenze e le abilità necessarie per svolgere i compiti richiesti dal lavoro di cybersecurity".

Tale gruppo comprende "funzioni tecniche e non tecniche che vengono svolte da dipendenti con conoscenze ed esperienze".

Tuttavia, è difficile creare una forza lavoro con le necessarie competenze interdisciplinari e risolvere il problema della comunicazione tra educatori, ricercatori e persone che utilizzano le tecnologie

dell'informazione.

È necessaria la cooperazione e la comunicazione tra questi gruppi.

Un problema è che le aziende, soprattutto le PMI con minori risorse, hanno bisogno di aiuto per valutare le competenze e le lacune dei propri dipendenti, utilizzando metodi digitali per migliorare la situazione esistente e organizzando opportunità di formazione per riqualificare i propri dipendenti.

Formazione e tutoraggio

Gli imprenditori, compresi quelli del futuro, hanno bisogno di modi di pensare complessi e della capacità di comprendere e integrare conoscenze provenienti da settori diversi, il che richiede un apprendimento interdisciplinare.

I problemi ingegneristici complessi richiedono la creazione di una situazione interdisciplinare in modo quasi naturale.

In un approccio interdisciplinare, gli studenti devono integrare le informazioni provenienti da diverse discipline e campi.

Sviluppano una comprensione interdisciplinare, imparano a integrare le aree di competenza e i modi di pensare specifici della disciplina.

In questo modo si incrementano le capacità cognitive e il pensiero critico più che con i singoli mezzi disciplinari.

Ingegneria sociale

- significa manipolare gli esseri umani (spesso utilizzando metodi psicologici) per ottenere l'accesso a dati, documenti e informazioni di interesse per l'attaccante.
- è oggi una delle principali minacce alla sicurezza informatica e rappresenta una forma efficace di criminalità informatica.
- potrebbero avere pericolose ripercussioni, ad esempio la violazione dei dati, più di qualsiasi altro tipo di attacco.
- gli attacchi hanno uno scopo finanziario e quindi le organizzazioni hanno perso notevoli somme di denaro.
- è particolarmente pericoloso perché si basa più sull'errore umano che sulle vulnerabilità del software e dei sistemi operativi.

Le aziende:

- potrebbero subire una perdita di produttività, un calo del morale dei dipendenti e difficoltà di recupero.
- hanno un danno di reputazione perché i clienti non sono convinti che l'organizzazione sia in grado di proteggersi.
- Spesso è necessario innescare una vecchia risposta agli incidenti.
- dovrebbero fornire un software di sicurezza che aiuti a prevenire attacchi futuri.
- spesso devono riqualificare i dipendenti per essere pronti agli attacchi.

Formazione sull'ingegneria sociale (consapevolezza informatica)

- di dipendenti e manager per i quali è importante riconoscere gli attacchi di social engineering perché il rischio di diventarne vittima è elevato.
- potrebbero essere inclusi nei programmi di sensibilizzazione alla sicurezza della comunità, dei singoli e dei cittadini e proteggere gli individui e la loro organizzazione.
- è particolarmente carente nelle PMI che dispongono di minori risorse, per cui dovrebbero essere aiutate a prendere sul serio la formazione sulla consapevolezza informatica e a offrire ai dipendenti l'opportunità di seguirla.

Il ciclo di vita degli attacchi di ingegneria sociale

Attaccante:

- per prima cosa indagano sulla vittima presa di mira per raccogliere le informazioni di base necessarie, come i punti di ingresso e i protocolli di sicurezza deboli, necessari per l'attacco.
- poi tentare, guadagnare la fiducia della vittima e fornire incentivi per azioni che di solito non sono pratiche di sicurezza, come la divulgazione di informazioni sensibili o la concessione dell'accesso a risorse critiche.

La Figura 2 spiega il ciclo di vita di un attacco.

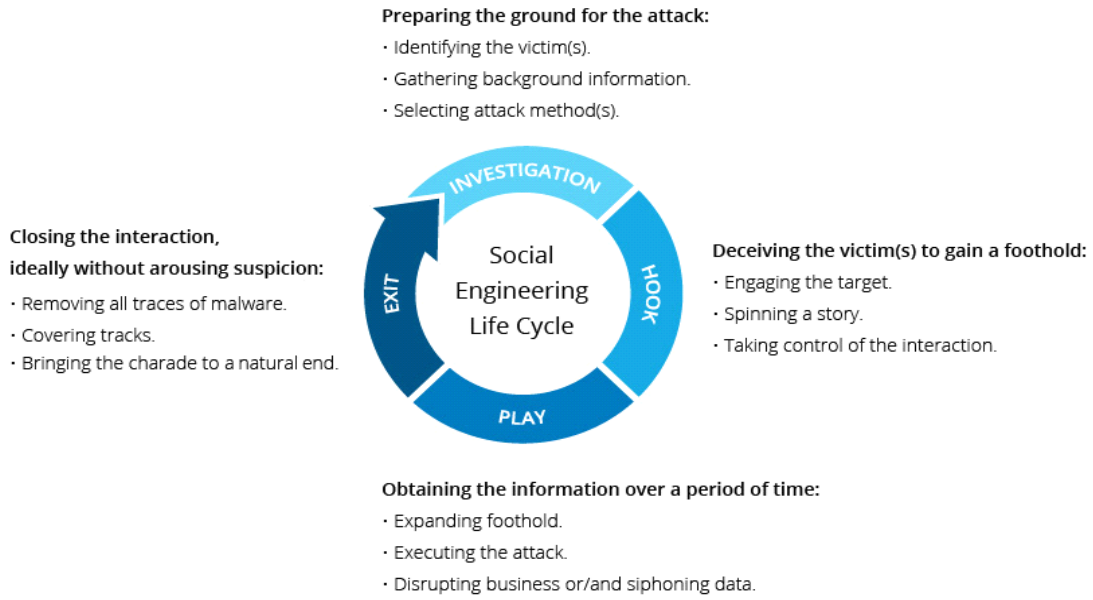

Figura 2: Ciclo di vita di un attacco

Social networks

- è diventato molto popolare negli ultimi anni, offrendo agli utenti una piattaforma per comunicare con la famiglia, gli amici e i colleghi.
- e Social Networking si riferisce all'uso di siti di social networking basati su Internet per connettersi e comunicare con amici, familiari, colleghi, clienti o clienti.
- hanno i loro server in centri dati ubicati presso i principali punti di accesso alla rete Internet.

La figura 3 mostra alcune aree in cui i social media svolgono un ruolo importante:

- Intrattenimento
- costruire opportunità di business
- per fare carriera
- migliorare le abilità sociali
- sviluppare relazioni con altri individui

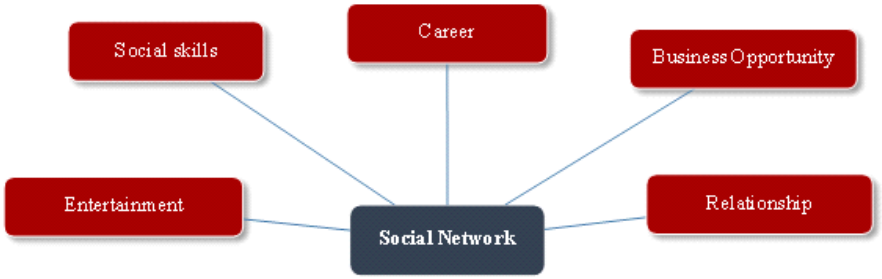

Figura 3: Ruoli nella rete sociale

Un social network:

- è una base per i marketer che cercano clienti per aumentare il riconoscimento del marchio, promuovere la fedeltà al marchio, migliorare i tassi di conversione, fornire l'accesso e il coinvolgimento di nuovi, recenti e vecchi clienti.
- rende possibile, attraverso la condivisione di post, immagini, video o commenti sui social network, che più persone visitino il sito web dell'azienda e diventino clienti.
- rende difficile stare al passo con i cambiamenti e influisce anche sul tasso di successo del marketing di un'azienda.

I siti di social networking (social media) più popolari negli Stati Uniti e in Europa sono:

- Facebook
- Instagram
- Twitter
- YouTube
- WhatsApp
- LinkedIn (di stampo più professionale, aiuta a mettere in contatto i professionisti con colleghi, contatti di lavoro e datori di lavoro)

Il social networking si basa sullo sviluppo e sul mantenimento di relazioni personali e aziendali utilizzando la tecnologia e i siti di social networking (Social Media) che consentono alle persone e alle aziende di connettersi tra loro, sviluppando relazioni, condividendo informazioni, idee e messaggi.

I membri della famiglia possono rimanere in contatto attraverso social network personali come Facebook, condividere foto e inviare altri messaggi sulla loro vita.

Le persone possono anche entrare in contatto con altri (sconosciuti) che condividono gli stessi interessi.

I social media presentano anche degli svantaggi, tra cui la diffusione della disinformazione e gli elevati costi di utilizzo e mantenimento dei profili sui social media.

Le funzionalità delle piattaforme sociali possono essere classificate in:

Le funzioni di rete servono a promuovere le relazioni sociali tra gli utenti all'interno delle piattaforme virtuali e forniscono funzionalità per la costruzione e il mantenimento del grafo della rete sociale.

Le funzioni dati sono responsabili della gestione dei contenuti forniti dagli utenti e della

comunicazione tra gli utenti, contribuendo a migliorare (estendere) l'interazione con gli utenti e a rendere la piattaforma più attraente.

Le funzioni di controllo dell'accesso mirano a implementare misure di privacy definite dall'utente e a limitare l'accesso non autorizzato ai dati e alle informazioni fornite dall'utente.

Vantaggi e svantaggi dei social network

Vantaggi

I social media consentono alle aziende di:

- entrare in contatto con clienti nuovi ed esistenti.
- essere in grado di creare, promuovere e aumentare la consapevolezza del marchio.
- affidarsi alle recensioni e ai commenti dei propri clienti, importanti per aumentare le vendite del marchio e il posizionamento sui motori di ricerca.
- essere in grado di stabilire un nuovo marchio. dimostrare un alto livello di servizio ai propri clienti.
- poter migliorare i prodotti e le relazioni con i consumatori.

Svantaggi

- possono contribuire alla diffusione della disinformazione.
- possono avere un impatto negativo sulle aziende perché le critiche a un marchio si diffondono molto rapidamente sui social media.
- richiedono ore di lavoro e costi settimanali per costruire e mantenere un profilo aziendale.

Sicurezza e privacy nelle reti sociali

- Le informazioni condivise sui social network e sui media si diffondono molto rapidamente, il che rende interessante per gli aggressori acquisirle.
- Le questioni di sicurezza e di privacy relative alle informazioni condivise dall'utente, quando quest'ultimo carica contenuti personali come foto, video e audio, devono essere rispettate perché l'aggressore può utilizzare le informazioni condivise per scopi illegittimi.
- La mancanza di consapevolezza degli utenti in materia di sicurezza e privacy può potenzialmente portare a vari attacchi informatici attraverso i social media.

Le minacce possono essere suddivise in tre categorie:

- Le minacce convenzionali comprendono quelle che gli utenti hanno incontrato fin dall'inizio del social network.

- Le minacce moderne sono attacchi che utilizzano tecniche avanzate per compromettere gli account utente.
- Gli attacchi mirati sono attacchi rivolti a un utente specifico, che possono essere commessi da qualsiasi utente per varie vendette personali.

Soluzioni per gli operatori di social network

- Sono state proposte procedure di autenticazione come CAPTCHA, autenticazione a più fattori e identificazione fotografica degli amici.
- Impostazioni di sicurezza e privacy per consentire al cliente di inserire le informazioni personali da accessi indesiderati da parte di estranei o applicazioni.

Le segnalazioni degli utenti di qualsiasi forma di abuso o di violazione delle norme da parte di qualsiasi utente della loro rete.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. Quali sono le vostre aspettative riguardo al progetto InCyT?
2. Come proteggersi dagli attacchi informatici
3. Che cos'è l'ingegneria sociale
4. Rete sociale (Social Media)

Domande di autovalutazione.

- Come proteggersi dagli attacchi informatici
- Che cos'è l'ingegneria sociale
- Rete sociale (Social Media)

Allegati

Presentazione di PowerPoint
Filmati

Riferimenti:

- InCyT - Formazione interdisciplinare in campo informatico

- Recupero degli incidenti informatici
- Ridurre al minimo gli attacchi informatici - Strategia di resilienza informatica
- Come prevenire i cyberattacchi: I modi migliori per proteggersi
- Sicurezza dei social media: quanto sono sicure le vostre informazioni?
- Controlli interni sui sistemi informativi
- L'adozione dei social media comporta nuovi rischi
- Sicurezza dei social media - 5 consigli per la sicurezza
- 19 Migliori pratiche di sicurezza dei social media