TEMATICI DE CURS PROPUSE
CURRICULĂ CURSURI PRE-UNIVERSITARE

1. Elemente introductive în securitatea cibernetică

Prezentare generală

În cadrul acestui curs, elevii se vor familiariza cu conceptele de bază, terminologiile şi tehnologiile folosite în domeniul securităţii cibernetice şi vor dobândi o imagine clară a abilităţilor necesare pentru a activa în acest domeniu.

Tematicile propuse reprezintă, în esenţă, un ghid de nivel începător pentru cei interesaţi de domeniul securităţii cibernetice, fără a fi necesar un background tehnic foarte bogat.

Module

1.1. Fundamentele securităţii cibernetice

- Concepte de bază
- Principiul Least Privillege
- Principiul CIA (Confidentiality Integrity Availability)
- Metode de autentificare

1.2. Securitatea reţelelor

- noțiuni de baza (IP, gateway, conectare la internet, DNS, porturi)

1.3. Introducere în criptografie

- noțiuni de baza (configurare router, algoritmi principali)

1.4. Tipuri de atacuri

- Malware
- Phising
- Web Application Attacks
- DoS şi DDoS
- Man-In-The-Middle

1.5. Tehnologii pentru asigurarea securităţii cibernetice

- Antivirus
- IPS/IDS
- VPN
- Firewall

Modalitate de desfăşurare:	*Predarea elementelor propuse de către* ***cadrele didactice – 4 ore***
Total ore tematică:	***4 ore / săptămână***

2. Securitatea cibernetică a sistemelor informatice

Prezentare generală

În contextul actual, în care sistemele informatice sunt supuse la multiple ameninţări, iar datele personale ale utilizatorilor sunt privite ca produse ce pot fi tranzacţionate pe piaţă, este necesar ca la nivelul sistemelor informatice să fie asigurată o minimă securitate şi să existe o informare a utilizatorilor în privinţa riscurilor existente.

Astfel, securitatea cibernetică trebuie privită din perspectiva rolului pe care sistemul îl are în cadrul infrastructurii (cerere de servicii, oferire de servicii, echipament de reţea), fiecare rol necesitând diferite soluţii şi metode de asigurare a securităţii.

Tematicile propuse prezintă diferitele roluri pe care un sistem le poate avea în cadrul unei reţele şi modalităţile în care poate fi securizat, dar şi metodele prin care poate fi compromis.

Module

2.1. Definiţia unui sistem informatic

- Funcţionalităţi: client, server, echipament de reţea
- Plasarea în cadrul unei reţele

2.2. Asigurarea securităţii sistemului informatic la nivel de aplicaţie

- Metode implementate la nivelul sistemelor de operare pentru a preveni exploatarea

2.3. Asigurarea securităţii sistemului la nivel de reţea

- Asigurarea accesului la distanţă pentru sisteme informatice (Remote Desktop, VPN, SSH)
- Modalităţi de autentificare la nivel de reţea: politici pentru credenţiale, modalităţi de autentificare în doi paşi

2.4. Asigurarea securităţii sistemelor informatice la nivelul utilizatorului

- Campanii de awareness
- Instruirea utilizatorului referitor la tehnici de inginerie socială: phishing, mesaje de email cu documente ce conţin diverse modalităţi de infecţie vulnerabilităţi)
- Instruirea utilizatorului privind bune practici: asigurarea actualizărilor aplicaţiilor şi a sistemului de operare, credenţiale.

Modalitate de desfășurare:	▪ *Predarea elementelor propuse de către* ***cadrele didactice: 3 ore*** ▪ *Intervenție din partea* ***Centrului Național Cyberint: 1 oră***
Total ore tematică:	***4 ore / săptămână***

3. Securitatea cibernetică a dispozitivelor mobile

Prezentare generală

După revoluţia la nivel global oferită de accesul la Internet din anii 2000, după anul 2010 asistăm la revoluţia dispozitivelor mobile.

Migrarea pe echipamente mobile şi pătrunderea acestora în viaţa cotidiană, precum şi extinderea trend-ului BYOD (Bring your own device) şi BYOC (Bring your own cloud), aduce cu sine nevoia de securitate a datelor, precum şi o provocare pentru responsabilii IT.

Adopţia accelerată a mobilităţii la nivel global are un impact important asupra mediului enterprise, care se confruntă deja cu provocări sporite pe zona de securitate.

Totodă, protecţia datelor personale vehiculate în mediul mobil este o necesitate pentru fiecare utilizator, awareness-ul fiind un prim pas pentru o utilizare mai sigură a dispozitivelor mobile.

Module

3.1. Tipuri de sisteme de operare pentru dispozitivele mobile

- Android
- iOS
- Blackberry
- Windows

3.2. *Noțiune introductive:* Vulnerabilităţi ale sistemelor de operare mobile

- Rooting/Jailbreak
- Tipuri de malware
- Vulnerabilităţi wireless/bluetooth/NFC/GPS
- Vulnerabilităţile datelor din cloud

3.3. *Noțiune introductive:* Metode de securizare ale dispozitivelor mobile

- Elemente de securitate oferite de sistemele de operare mobile
- Criptarea
- Antiviruşi

Modalitate de desfăşurare:	▪ *Predarea elementelor propuse de către* ***cadrele didactice: 1 oră***
Total ore tematică:	***1 oră/săptămână***

4. Modalităţi de prevenţie în spaţiul virtual

Prezentare generală

Uneori suntem prezenţi în spaţiul virtual, chiar dacă nu suntem conştienţi de acest lucru, doar prin simplul fapt că deţinem sau interacţionăm cu echipamente "inteligente", care comunică GSM, bluetooth, WiFi sau NFC. Date pur statistice sau cu caracter confidenţial, legate de persoane fizice şi juridice sunt permanent generate, colecţionate, stocate şi comercializate.

Desigur, există limitări legale care reglementează unele dintre aceste aspecte, dar dincolo de acţiunile şi atribuţiile autorităţilor abilitate, este de datoria fiecăruia dintre noi să adoptăm o conduită preventivă în interacţiunea inevitabilă cu mediul virtual.

Doar cunoscând valoarea urmelor informatice generate de fiecare dintre noi, precum şi modul în care acestea pot fi utilizate fără acordul, dar mai ales în detrimentul nostru, vom putea prevedea în bună măsură posibile consecinţe mai puţin dorite.

Cursul prezintă diverse modalităţi de interacţiune voluntară sau involuntară cu spaţiul virtual, precum şi expunerea la o serie de riscuri şi vulnerabilităţi ce decurg din această situaţie.

Module

4.1. Conceptul de "spațiu virtual"

- Echipamente dotate cu tehnologie GSM, bluetooth, WiFi sau NFC - de la carduri bancare, la maşini de spălat şi automobile
- *Noțiuni generale*: Web, deep web, dark web
- Site-uri, forum-uri, aplicaţii
- Internet of Things

4.2. Elemente constitutive ale identităţii în spațiul virtual

- Profiluri şi identităţi fictive. Furtul de identitate.
- **Anonimizarea - iluzia anonimatului**
    - *Noțiuni generale*: Virtual Private Network

4.3. Legislaţie

- Legislaţie naţională şi internaţională
- Modalităţi de intervenţie
- Autorităţi competente

Modalitate de desfăşurare:	▪ *Predarea elementelor propuse de către* ***cadrele didactice: 2 ore***
Total ore tematică:	***2 ore/săptămână***

5. Managementul incidentelor de securitate cibernetică

Prezentare generală

Domeniul securității cibernetice a început să capete noi dimensiuni odată cu creșterea gradului de automatizare a nivelului tehnologic și extinderea și amplificarea amenințărilor/atacurilor cibernetice.

Administratorii de securitate din orice organizație au misiunea dificilă de a încerca să facă față tuturor amenințărilor cibernetice cu care se confruntă și de a minimiza posibilitățile de compromitere a infrastructurii IT. În acest sens, este necesar a fi optimizat procesul de monitorizare a evenimentelor de securitate, în scopul prevenirii, detecției și răspunsului la incidentele de securitate cibernetică.

Cursul prezintă etapele esenţiale de colectare a evenimentelor de securitate de la tehnologiile de securitate implementate în cadrul unei infrastructuri, alături de mecanismele şi instrumentele de monitorizare și analiză a incidentelor.

Module

5.1. Introducere în Cyber Defense

- Descrierea etapelor unui atac cybernetic - Kill Chain
- Atacuri tradiţionale vs. atacuri moderne
- Prezentare vectori de infecţie

5.2. Arhitectura de securitate a infrastructurilor cibernetice

Descrierea următoarelor tehnologii de securitate și prezentarea rolului lor în securizarea infrastructurilor din punct de vedere cibernetic

- Router
- Switch
- Firewall
- Proxy

Modalitate de desfășurare:	▪ *Predarea elementelor propuse de către* ***cadrele didactice: 2 ore***
Total ore tematică:	***2 ore/săptămână***

7. Investigaţii criminalistice IT&C - forensics

Prezentare generală

În situația producerii unui atac cibernetic, devin necesare răspunsurile la întrebările "5W" (Who, What, When, Where, Why?). Acestea se pot obține prin tactici, tehnici și proceduri specifice domeniului computer forensics, care presupun studierea artefactelor de la nivelul sistemelor informatice și ale echipamentelor de securitate afectate.

Modul de structurare al cursului este progresiv, în conformitate cu ordinea cronologică a procesului de investigare tehnică a unui incident de securitate cibernetică.

Modalitate de desfășurare:	▪ *Intervenție din partea* ***Centrului Național Cyberint: 1 oră***
Total ore tematică:	***1 oră/săptămână***

TOTAL ORE CURRICULĂ: 14 ore / semestru

OBSERVAȚIE: intervenția din partea universităților în cadrul orelor de curs va fi stabilită de către licee în funcție de disponibilitatea cadrelor universitare.