UNIVERSITATEA DE STAT DIN MOLDOVA

Facultatea de RelațiiInternaționale, ȘtiințePoliticeși Administrative

Programul de master: Studii de Securitate Națională

Lucru individual

“**Criminalitatea Cibernetică**”

Profesor: Tatiana Busuncian

Doctor, conferențiar universitar

Autor: Gheorghe Friptu, gr.02, SSN

Chișinău, 2023

Criminalitatea cibernetică devine, pe zi ce trece, un pericol din ce în ce mai mare, iar calculatorul este un factor criminogen de prim ordin în acest sens ce pune la dispoziţia conduitei criminale atât un nou obiect cât şi un nou instrument. În contextual în care informaţia a devenit foarte valoroasă, tentaţiile de fraudare a sistemelor au devenit din ce în ce mai mari. Având ca motiv fie interese financiare sau de alt gen, fie pur şi simplu distracţia, infracţionalitatea şi-a găsit un loc bun şi în reţelele de calculatoare. În acest sens, prin natura sa necontrolată de vreo autoritate, comunicarea în Internet, reprezintă un mediu excelent de a exprima liber opiniile şi identitatea proprie. Acest lucru implică însăşi posibilitatea formării unor comunităţi, ale căror preocupări nu sunt dintre cele mai paşnice. Astfel, persoanele interesate de piraterie software, audio/video-pornografie sau de accesul neautorizat la sistemele de calcul îşi pot uşor găsi parteneri cu preocupări similar între ceilalţi utilizatori. Comunicarea lipsită de bariere le permite celor experimentaţi în activităţi ilegale să le transmit celorlalţi cunoştinţele lor. De multeori, aceştia din urmă doresc să îşi demonstreze capacităţile nou-dobândite pentru a obţine recunoaştere şi a fi acceptaţi de comunităţile „experimentaţilor”, astfel fiind o dată în plus motivaţi în a comite infracţiuni informatice. Sistemele de calcul sunt în general protejate de accesul persoanelor neautorizate. Există mai multe mecanisme de autentificare şi apoi autorizare a utilizatorilor, însă cel mai răspândite sunt cele bazat pe nume de utilizator şi parolă (username şi password). Drept urmare la cele expuse mai sus, infracţionalitatea cibernetică include următoarele categorii de autori:

**hackeri** – persoane, mai ales tineri, care pătrund în sistemele informatice din motive legate de provocare intelectuală sau de obţinerea şi menţinerea unui anumit statut în comunitatea prietenilor;

**spioni** – persoane care pătrund în sistemele informatice pentru a obţine informaţii care să le permit câştiguri de natură politică;

**terorişti** – persoane care pătrund în sistemele informatice cu scopul de a provoca teamă, precum şi în scopuri politice;

**atacatori cu scop economic** – pătrund în sistemele informatice ale concurenţilor comerciali, cu scopul de a obţine câştiguri financiare, în interesul altor persoane; **criminali de profesie** – pătrund în sistemele informatice ale întreprinderilor pentru a obţine câştig financiar, în interes personal;

**vandali** – persoane care pătrund în sistemele informatice cu scopul de a cauza pagube.

Astfel, în lumea virtual există anumite etape ale avansării de la un simplu utilizator la autorul unei fapte infracţionale.

În aceste situaţii **novicele** este de obicei un începător singuratic. Nu are experienţă în calculatoare şi nici cum să pătrundă în sisteme din afară. Novicele lucrează singur şi nu are ajutor, fiind de cele mai dese ori un experimentator care nu comite ilegalităţi.

**Ucenicul** este acel novice care progresează dincolo de fazele iniţiale, în general cu ajutorul internetului, schimbând mesaje cu cei care i se aseamănă, astfel nu numai că îşi îmbunătăţeşte considerabil cunoştinţele, dar devine parte a unei reţele. El învaţă să îşi acopere mai bine urmele şi să intre sau să iasă din sisteme informatice fără să atragă atenţia.

**Vizitatorul** este, probabil, cel mai „inocent” dintre atacatori. Această persoană este un simplu trecător curios. Rareori se întâmplă ca el să compromită sistemele, în afara cazului în care întâlneşte o oportunitate serioasă.

**Amatorul** avansat sau, altfel spus, semi-profesionistul, spre deosebire de vizitator, este greu de detectat şi de cele mai dese ori are o dorinţă specială de a face rău. Pentru mulţi din această categorie scopul principal este să vadă cât de mult pot distruge.

**Profesionistul** este diferit de toate celelalte categorii de intruşi: este o persoană bine antrenată, un spion profesionist al calculatoarelor. Aceste persoane se pricep foarte bine să intre într-un sistem de calcul şi să îl părăsească fără să fie observaţi în vreun fel.

Conform ultimelor date analizate se aratăcă, până în 2025, costurile generate de criminalitatea cibernetică vor ajunge la 10,5 trilioane de dolari la nivel mondial, de la 3 trilioane dolari în 2015, reprezentând una dintre cele mai profitabile activităţi infracţionale.

Criminalitatea cibernetică poate lua mai multe forme:

* Accesul neautorizat la sistemele sau reţelele de calculatoare în scopul furtului de informaţii sensibile, al întreruperii operaţiunilor sau răspândirii de programe malware;
* Înşelarea persoanelor pentru a le convinge să furnizeze informaţii sensibile, cum ar fi datele de autentificare, detaliile cardului de credit sau informaţii personale prin intermediul unor e-mailuri, site-uri web sau conturi de socializare false;
* Utilizarea informaţiilor personale furate pentru a comite fraude, a deschide conturi sau a face achiziţii;
* Înşelarea persoanelor pentru a trimite bani sau furniza informaţii personale prin reclame online false, postări pe reţelele de socializare sau e-mailuri.

Criminalitatea informatică poate afecta persoanele fizice, companiile şi guvernele. Aceasta poate avea ca rezultat, printer altele, pierderi financiare, afectarea reputaţiei, pierderea proprietăţii intelectuale. Infractoriici bernetici pot proveni de oriunde din lume şi, de cele mai multe ori, acţionează în mod anonim. Acest lucru face dificilă identificarea şi, ulterior, urmărirea penală a acestora de către autorităţile publice. Multe ţări dispun de legi pentru a combate criminalitatea informatică, dar aplicarea şi urmărirea penală pot fi dificile. În consecinţă, măsurile preventive cum ar fi utilizarea unor parole puternice, actualizarea programelor informatice şi precauţia faţă de e-mailurile şi site-urile suspecte sunt esenţiale şi pot contribui la protecţia împotriva criminalităţii informatice. În plus, organizaţiile pot implementa protocoale de securitate cibernetică şi pot investi în formarea angajaţilor pentru a reduce riscul de atacuri cibernetice. Cu toate acestea, în cazul în care se întâmplă un atac, reacţia rapidă şi implicarea unor profesionişti care ştiu cum să abordeze astfel de incidente sunt esenţiale şi presupun:

1. Raportarea incidentului: Dacă sunteţi victim unei infracţiuni informatice, este important să raportaţi incidental autorităţilor competente. Printre acestea se pot număra autorităţile locale, agenţiile naţionale de securitate cibernetică sau organizaţii internaţionale precum Interpol;

2. Colectarea probelor: Este important să se colecteze şi să se păstreze dovezile atacului cibernetic, cum ar fi fişierele, traficul de reţea şi orice e-mailuri sau mesaje legate de incident. Acest lucru poate ajuta la identificarea autorilor şi poate oferi dovezi pentru urmărirea penală;

3. Izolarea incidentului: Odată ce un incident a fost detectat, este important să fie izolat pentru a preveni alte daune. Acest lucru poate implica izolarea sistemelor infectate, închiderea reţelelor sau blocarea traficului maliţios;

4. Recuperarea în urma incidentului: După izolarea incidentului, următorul pas este recuperarea. Acest lucru poate implica restaurarea datelor din copiile de rezervă, repararea sau înlocuirea sistemelor deteriorate şi implementarea unor măsuri de securitate suplimentare pentru a preveni incidente viitoare;

5. Analize si măsuri post incident: În cele din urmă, este important să se înveţe din incident şi să se îmbunătăţească practicile de securitate cibernetică pentru a preveni incidente similar în viitor. Acest lucru poate implica efectuarea unei analize post-incident, identificarea domeniilor de îmbunătăţire şi implementarea unor măsuri noi şi protocoale de securitate.

În concluzie subliniem că crimele cibernetice capătă tot mai mult character transnaţional, organizaţional şi de grup. Odată cu utilizarea reţelei globale Internet, astfel de infracţiuni nu mai au hotare. Ele pot fi comise fără a ieşi din casă sau din oficiu, din sistemul de calcul al unui stat la adresa subiecţilor altui stat, iar datele ce se conţin în sistemele de calcul pot fi de scurtă durată – ceea ce dă posibilitate infractorului să evite pedeapsa.

În lupta cu criminalitatea cibernetică este nevoie de un cadru legislativ bine pus la punct în ceea ce priveşte prevenirea, descoperirea şi sancţionarea acestor fapte.