Protecția informației. Prevenirea și curmarea fraudelor informatice

Autor: Tatiana Busuncian

Dr., conferențiar universitar

Chișinău 2023

Conținuturi, Obiective de referință

Obiective de referință:

- să definească caracteristicile securității informaționale;
- să determine instrumentele şi metodele de luptă cu amenințările cibernetice;
- să evalueze motivele criminalității cibernetice şi să descrie eforturile întreprinse pentru asigurarea securității informaționale şi de securitate națională, în general;
- să estimeze importanța prevenirii amenințărilor complexe și persistente la adresa securității informaționale.

Termeni-cheie: *securitate informațională, știri false, mediului informaţional, pericol, politică.*

Asigurarea securității informaționale

→ Spațiul informațional reprezintă o platformă confortabilă pentru pregătirea şi efectuarea crimelor informatice, a actelor de terorism cibernetic şi a altor acțiuni malițioase, menite să afecteze, direct sau indirect, securitatea națională.

Penetrarea sistemelor informaționale sau de comunicații electronice ale autorităților administrației publice şi ale altor instituții şi întreprinderi de stat sau private, în cadrul cărora se gestionează informație sensibilă, poate duce la compromiterea confidențialității, integrității sau disponibilității acestei informații, şi, prin urmare, la cauzarea prejudiciilor financiare sau de altă natură, inclusiv la afectarea securității statului.

Ce ține de Republica Moldova, penetrarea sistemelor informatice aferente infrastructurii critice poate duce la obținerea controlului neautorizat asupra acestor sisteme, şi, în consecință, la afectarea proceselor economice, sociale, politice, informaționale, militare etc.

Asigurarea securităţii informaţionale

→ Misiunile primordiale în prevenirea şi combaterea agresiunilor din mediul virtual, intern sau extern sunt îndreptate spre sistemele informatice şi de comunicaţii electronice de importanţă statală. Aceste misiuni sunt realizate, în conformitate cu legislaţia în vigoare, prin intermediul unor procese operaţionale cum ar fi:

- elaborarea propunerilor privind asigurarea securităţii informatice, elaborarea şi promovarea politicii de stat şi exercitarea controlului în domeniul asigurării protecţiei informaţiei atribuite la secretul de stat în spaţiul cibernetic;
- crearea, asigurarea funcţionării şi securităţii sistemelor guvernamentale de comunicaţii electronice, elaborarea strategiei şi realizarea politicii naţionale în domeniul creării, administrării şi asigurării funcţionării şi securităţii sistemelor speciale de comunicaţii electronice;
- asigurarea conducerii ţării, a ministerelor, departamentelor şi a altor autorităţi publice, inclusiv şi în străinătate, conform Nomenclatorului întocmit de Guvern, cu legătură guvernamentală, cifrată, secretă şi cu alte tipuri de telecomunicaţii, organizarea şi asigurarea siguranţei exploatării lor;
- depistarea emiterilor radio ale mijloacelor radioelectronice emiţătoare a căror activitate periclitează securitatea de stat.

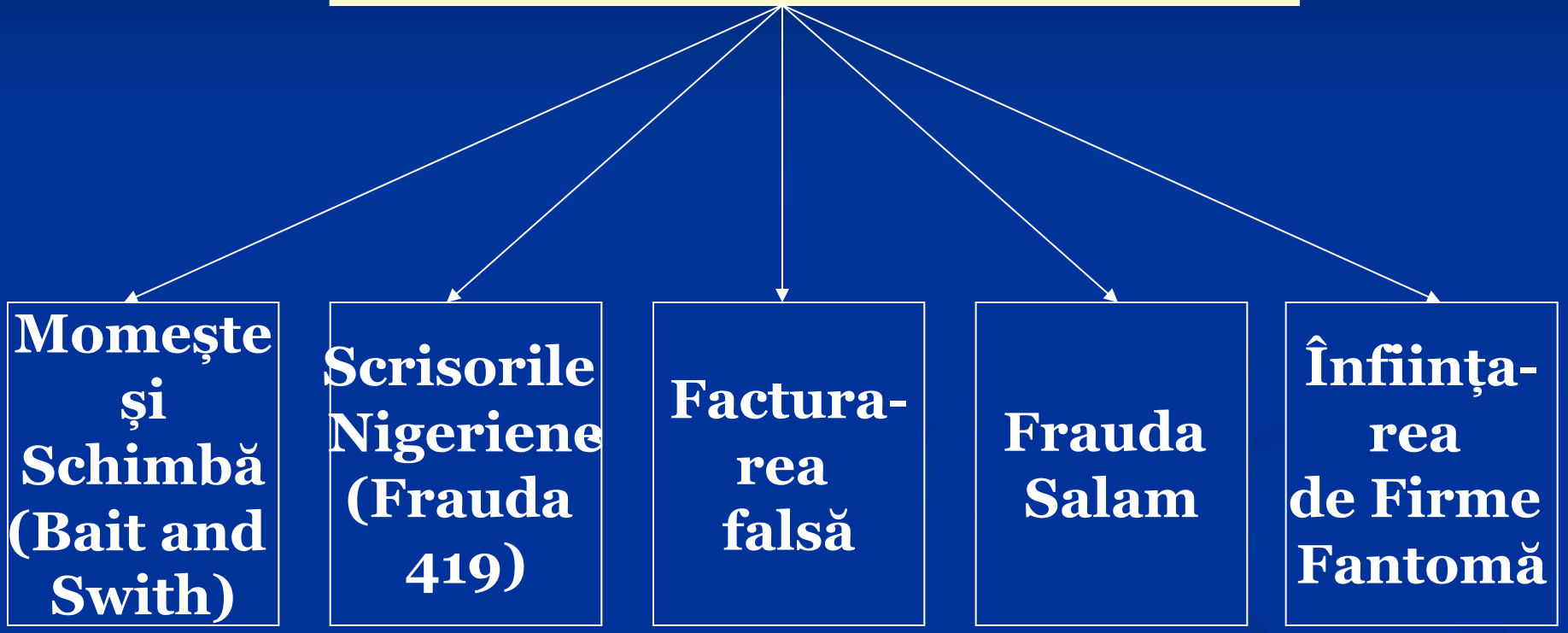
Fraudele informatice: consideraţii generale

→ **Fraudele informatice** reprezintă „orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoarea este instrumentul sau mediul de înfăptuire a unei infracţiuni”.

→ **În sens restrîns:** „orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor”.

- *„Orice incident legat de tehnica informatică în care o victimă a suferit sau ar fi putut să sufere un prejudiciu și din care autorul a obținut sau ar fi putut obține intenționat un profit.”*
- *„Orice acțiune ilegală în care un calculator constituie instrumentul sau obiectul delictului, sau, altfel spus, orice infracțiune al cărei mijloc sau scop este influențarea funcției calculatorului (funcționării normale a calculatorului).”*

Formele fraudelor informatice



Momește și schimbă

- Este o formă de fraudă informatică în care făptuitorul ademenește potențiali clienți făcând publicitate unor produse, care fie nu există în realitate, fie sunt ulterior schimbate cu produse aparent similare, dar cu calitțăi net inferioare.
- Fapta se realizează cel mai adesea prin intermediul sistemelor informatice și al rețelei Internet. Ademenirea clienților se poate face și prin mesaje de poștă electronică sau prin intermediul unei pagini de Web.

Scrisorile nigeriene

- Sunt adesea cunoscute sub denumirea de „transferuri nigeriene” sau „Fraude cu avans” ori, pur si simplu, „înșelătorii 419” (după Codul Penal al Nigeriei se încriminează astfel de fapte).
- În acest caz, victimele sunt oameni bogați sau investitori din Europa, Asia Australia sau America de Nord iar mijloacele de comitere variază de la scrisorile expediate prin poștă sau faxuri la email sau pagini web, în special dupa 1990.
- Astfel de înșelăciuni își au originea în Nigeria și, de regulă, sunt pregătite astfel încât adresele de email, site-urile Web, numerele de telefon sau fax etc. să pară a fi cele ale unor centre de afaceri, firme sau chiar instituții guvernamentale locale.

Depozite false

- O altă metodă de fraudare în sisteme informatice prin care, autorul după ce câștiga o licitație de produse pe un site Internet specializat (gen eBay), solicită victimei utilizarea unui site de escrow „sigur”, „neutru” care să „depoziteze” bunurile (produsele – în general echipamente electronice) pâna la perfectarea aranjamentelor financiare.

  Bineînteles, site-ul de escrow este creat și controlat de infractor, iar la primirea bunurilor „în gaj”, respectiva pagină Web este închisa (dezactivată) iar contul șters.

Mailbombing

Este considerată cea mai veche metodă de atac, deși esența sa este simplă și primitivă: un număr mare de mesaje de e-mail fac imposibilă lucrul cu cutiile poștale și, uneori, cu servere de mail întregi.

Multe programe au fost dezvoltate în acest scop și chiar și un utilizator neexperimentat ar putea efectua un atac specificând doar e-mailul victimei, textul mesajului și numărul de mesaje necesare.

Multe astfel de programe au făcut posibilă ascunderea adresei IP reale a expeditorului, folosind un server de e-mail anonim pentru e-mail. Acest atac este ușor de prevenit, deoarece majoritatea ISP-urilor au filtre anti-spam bune. Furnizorul poate limita numărul de scrisori de la un expeditor, iar un astfel de atac devine ineficient.

Selectarea parolei

- Următorul tip de atac este, de asemenea, simplu. Crackerul ridică parole pentru sistemele de control al accesului. La urma urmei, este destul de evident că utilizatorii de sisteme de calcul nu sunt de obicei capabili să țină cont de combinații de litere, cifre și semne lungi de până la o sută de caractere.

  Parola medie pentru accesarea sistemului nu depășește, de obicei, opt caractere, iar uneori un cuvânt sau o dată este folosită ca parolă.

Selectarea parolei

Când folosiți o dată, este simplu, deoarece opt cifre sunt doar 100.000.000 de combinații posibile, fie primele, fie ultimele 4 cifre indicând anul și fiind undeva între 1900 și 2050. Celelalte două cifre indică luna, adică ele iau valori de la 1 la 12. Cifrele rămase iau valori de la 1 la 31 - zilele lunii. Aici puteți exclude și date precum 3102 (31 februarie), deoarece astfel de date sunt rar folosite.

În absența protecției împotriva parolelor de forță brută, nu va fi dificil să găsiți o dată de cod pentru un program mediu: atunci când sortați aproximativ 100 de parole pe secundă (nu este o problemă chiar și pentru un computer lent), va dura puțin. mai mult de unsprezece zile.

Selectarea parolei

Pentru fraze, totul este ceva mai complicat, deoarece chiar dacă luăm alfabetul englezesc de 26 de litere (român - 31 de litere), atunci o frază de opt caractere va consta deja din 208.827.064.576 de opțiuni (1.406.408.618.241 de opțiuni pentru limba romina. Dar aici ingeniozitatea vine în ajutor: este puțin probabil ca utilizatorul să-și amintească secvențe aleatorii de caractere, adică este suficient să sortați toate cuvintele existente în dicționarul englez, dintre care nu vor fi mai mult de 200.000, inclusiv jargon și cuvinte rare, iar acest lucru este deja de un milion de ori mai simplu.

În plus, dacă începi să te gândești și mai atent, majoritatea cetățenilor, și pe lângă asta, cei care lucrează într-un anumit domeniu, au mult mai puține cuvinte în vocabular, ceea ce reduce numărul de opțiuni posibile cu un ordin de mărime. De asemenea, puteți lua în considerare că numele rudelor, animalelor de companie, numele orașelor pot fi folosite ca parole.

Selectarea parolei

Cu toate acestea, nu există niciun motiv să vă bazați pe o modalitate atât de ușoară de a obține o parolă. În prezent, majoritatea utilizatorilor (și cu atât mai mult administratorii de sistem ai companiilor comerciale) folosesc ca parolă secvențe aleatorii de caractere latine mari și mici, intercalate cu numere. Există mai multe moduri de a crea (și de a reține) o parolă puternică.

De exemplu, din primele litere ale expresiei „există un stejar verde lângă malul mării, un lanț de aur pe acel stejar”, se obține o parolă de 9 litere uldzzzndt, a cărei selecție va dura câteva trilioane de încercări.

Viruși, troieni, viermi de corespondență, sniffer, rootkit-uri și alte programe speciale

Următorul tip de atac este o metodă mai sofisticată de a obține acces la informații clasificate - aceasta este utilizarea de programe speciale pentru a lucra pe computerul victimei.

Astfel de programe sunt concepute pentru a căuta și a transfera informații secrete către proprietarul lor sau pur și simplu pentru a dăuna sistemului de securitate și performanței computerului victimei. Principiile de funcționare ale acestor programe sunt diferite, așa că nu le vom lua în considerare în această prezentare.

Inteligența rețelei

- În timpul unui astfel de atac, hackerul nu efectuează de fapt nicio acțiune distructivă, dar, ca urmare, poate obține informații confidențiale despre construcția și principiile de funcționare a sistemului informatic al victimei. Informațiile obținute pot fi folosite pentru a construi în mod competent atacul viitor și se face de obicei în etapele pregătitoare.
- În cursul unei astfel de recunoașteri, un atacator poate efectua scanări de porturi, interogări DNS (Domain Name System),
- ping porturi deschise, prezența și securitatea serverelor proxy. Ca urmare, puteți obține informații despre adresele DNS existente în sistem, cine le deține, ce servicii sunt disponibile pe acestea, nivelul de acces la aceste servicii pentru utilizatorii externi și interni.

Sniffing pachetelor

Este, de asemenea, un tip de atac destul de comun bazat pe funcționarea unei plăci de rețea în modul promiscuu. În acest mod, toate pachetele primite de placa de rețea sunt trimise pentru procesare către o aplicație specială pentru procesare.

Drept urmare, un atacator poate obține o cantitate mare de informații de serviciu: cine a trimis pachete de unde până unde, prin ce adrese au trecut aceste pachete.

Cel mai mare pericol al unui astfel de atac este obținerea de informații în sine, cum ar fi login-urile și parolele angajaților, care pot fi folosite pentru a intra ilegal în sistem sub masca unui angajat obișnuit al companiei.

IP-spufing

De asemenea, un tip obișnuit de atac în rețelele insuficient de sigure, atunci când un atacator își uzurpă identitatea unui utilizator autorizat, în timp ce se află în cadrul organizației în sine, sau în afara acesteia.

Pentru a face acest lucru, hackerul trebuie să folosească o adresă IP care este permisă în sistemul de securitate al rețelei.

Un astfel de atac este posibil dacă sistemul de securitate permite identificarea utilizatorului doar prin adresa IP și nu necesită confirmări suplimentare.

Man-in-the-Middle

Din engleza. "Bărbatul din mijloc" Un tip de atac când un atacator interceptează canalul de comunicație între două sisteme și obține acces la toate informațiile transmise. Obținând acces la acest nivel, un hacker poate modifica informațiile în modul în care dorește să-și atingă obiectivele.

Scopul unui astfel de atac este de a fura sau de a falsifica informațiile transmise sau de a obține acces la resursele rețelei. Astfel de atacuri sunt extrem de greu de urmărit, deoarece atacatorul se află de obicei în interiorul organizației.

Injecție

- Un atac de injecție implică introducerea unor comenzi sau date terță parte într-un sistem care rulează pentru a schimba cursul sistemului și, ca urmare, a obține acces la funcții și informații închise sau pentru a destabiliza sistemul în ansamblu. Un astfel de atac este cel mai popular pe Internet, dar poate fi efectuat și prin linia de comandă a sistemului.

SQL-injectiea

- Injecția SQL este un atac în care parametrii interogărilor SQL către baza de date sunt modificați. Ca urmare, cererea capătă un sens complet diferit și este capabilă nu numai să afișeze informații confidențiale, ci și să modifice / șterge date. Foarte des, acest tip de atac poate fi văzut pe exemplul site-urilor care utilizează parametrii de linie de comandă (în acest caz, variabile URL) pentru a construi interogări SQL împotriva bazelor de date fără o validare adecvată.

  Injecția PHP este o modalitate de a pirata site-urile care rulează pe PHP. Constă în executarea codului necesar pe partea de server a site-ului.

  Cross Site Scripting sau XSS (abreviar din engleză Cross Site Scripting) este un atac similar cu injecția SQL, dar pentru a efectua acest atac, un hacker nu modifică interogarea SQL, ci variabilele interne ale sistemului de operare (de exemplu, PHP, Perl etc.), folosind deficiențe în procesarea parametrilor de intrare a scripturilor sau erori în configurarea aplicațiilor de procesare a scripturilor.

Inginerie sociala

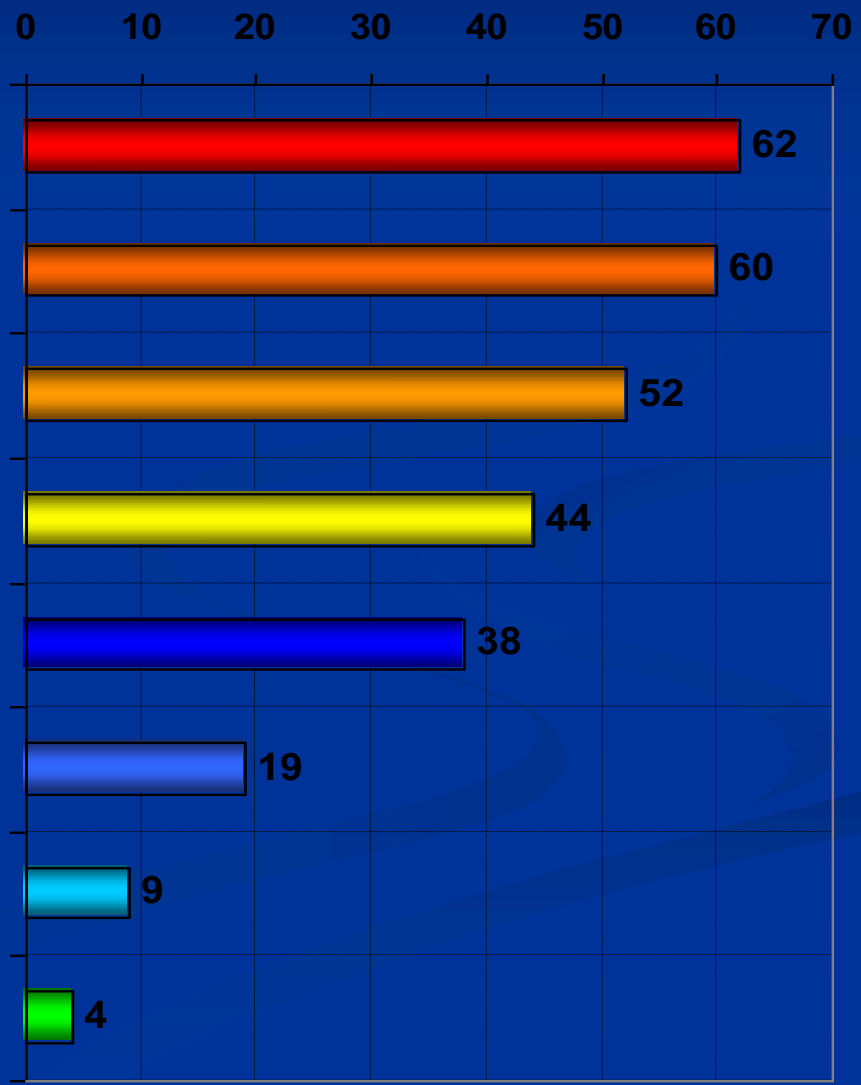
Ingineria socială (din engleză Social Engineering) este utilizarea incompetenței sau neglijenței personalului pentru a obține acces la informații. Această metodă este de obicei folosită fără computer, folosind un telefon obișnuit, poștă sau un pahar de bere.

În acest fel, se obține de obicei o mare varietate de informații. În cursul unui astfel de atac, hackerul stabilește contactul cu victima și, inducând în eroare sau câștigând încredere, încearcă să obțină informațiile necesare care sunt greu de obținut în alt mod, sau alte moduri care sunt mai riscante.

După cum spune vechea vorbă: „Cea mai slabă verigă dintr-un sistem de securitate este Omul”.

Cele mai periculoase amenințări IT

- Acțiuni din interior
- Programe malware
- Atacurile hackerilor
- Neglijența angajaților
- Spam
- Eșecuri hardware și software
- Furtul de echipamente
- Fraudă financiară



Subiecții fraudei informatice

Subiectul activ – poate fi orice persoană care răspunde penal

Subiectul pasiv- persoana fizică sau juridică, proprietară sau utilizatoare a sistemului informatic accesat ilegal sau a datelor informatice vizate

Raportul Comitetului European pentru probleme criminale evidențiază următorele categorii de fraude informatice:

- Infracțiunea de fraudă informatică;
- Infracțiunea de fals în informatică;
- Infracțiunea de prejudiciere a datelor sau programelor informatice;
- Infracțiunea de sabotaj informatic;
- Infracțiunea de acces neautorizat la un calculator;
- Infracțiunea de interceptare neautorizată;

- Infracțiunea de reproducere neautorizată a unei topografii;
- Infracțiunea de reproducere neautorizată a unui program informatic protejat de lege;
- Infracțiunea de alterare fără drept a datelor sau programelor informatice;
- Infracțiunea de spionaj informatic;
- Infracțiunea de utilizare neautorizată a unui calculator;
- Infracțiunea de utilizare neautorizată a unui program informatic protejat de lege.

Manualul Natiunilor Unite pentru prevenirea si controlul infracționalității informatice:

- Fraude prin manipularea calculatoarelor electronice
- Fraude prin falsificarea de documente
- Alterarea/modificarea programelor din calculator
- Accesul neautorizat la sisteme informatice
- Reproducerea neautorizata a programelor pentru calculator protejate de lege.

Fraudele informatice după rolul avut de sistemele informatice:

Infracţiuni săvârşite cu ajutorul sistemelor informatice, în care sistemele informatice constituie un instrument de facilitare a comiterii infracţiunilor. Este vorba despre infracţiuni tradiţionale, perfecţionate prin, Utilizarea sistemelor informatice

Infracţiuni săvârşite prin intermediul sistemelor informatice, în care sistemele informatice, incluzînd şi datele stocate în acestea, constituie ţinta infracţiunii.

OECD(Organizația pentru Cooperare și Dezvoltare)

Organizaţia pentru Cooperare Economică şi Dezvoltare (OECD) a fost una dintre primele organizaţii internaţionale care a realizat un studiu privind armonizarea legislaţiei în domeniu. În anul 1983, OECD a publicat un raport prin care a propus diferite recomandări legislative statelor membre ale Uniunii Europene precum şi o minimă listă de activităţi care trebuie pedepsite: fraudarea şi falsificarea realizată prin calculator, alterarea programelor de calcul şi a datelor, copyright-ul, interceptarea comunicaţiilor sau a altor funcţii a unui calculator, accesul şi utilizarea neautorizată a unui calculator

ONU (Organizația Națiunilor Unite)

Organizaţia Naţiunilor Unite s-a implicat, la rândul său, în studiul şi combaterea fenomenului analizat. Au fost publicate numeroase documente, dintre care se remarcă: raportul - "Propuneri privind concertarea acţiunilor internaţionale privind combaterea oricărei forme de activitate criminală" (1985); Rezoluţia introdusă de reprezentantul Canadei privind combaterea criminalităţii pe calculator (1990); "Declaraţia Naţiunilor Unite privind principiile de bază ale justiţiei aplicabile victimelor abuzului de putere şi crimei" (1990); - raportul "Provocarea fără frontiere"

Consiliul Europei

În completarea raportului OECD, Consiliul Europei a iniţiat propriul studiu de caz pentru dezvoltarea cadrului legal privind combaterea criminalităţii informatice. Comisia de experţi în domeniul criminalităţii pe calculator a Consiliului a adoptat Recomandarea R(89)9 care reprezintă un ghid de acţiune şi pentru statele membre ale Uniunii Europene.

Infracţiunile informatice ar putea fi clasificate, potrivit recomandărilor Consiliului Europei (lista minimală), în opt categorii:

1) frauda informatică – constând în orice ingerinţă într-un sistem informatic care îi influenţează rezultatul, cauzând prin aceasta un prejudiciu, cu intenţia de a obţine un avantaj material pentru sine sau pentru altul;

2) falsul informatic;

3) fapte care prejudiciază datele sau programele pentru calculator;

4) sabotajul informatic;

5) accesul neautorizat;

6) intercepţia neautorizată;

7) reproducerea neautorizată a unui program de calculator protejat;

8) reproducerea neautorizată a unei topografii.

Problemele ridicate în cadrul reuniunilor internaţionale privind combaterea fraudelor informatice sunt următoarele:

- lipsa unui consens global privind definiţia “fraudelor informatice”;
- lipsa unui consens global privind motivaţia realizării acestor fapte;
- lipsa expertizelor din partea persoanelor autorizate aparţinând unor instituţii cu atribuţii de control în domeniu;
- inexistenţa unor norme legale adecvate privind accesul şi investigaţia sistemelor informatice, inclusiv lipsa normelor prin care pot fi confiscate bazele de date computerizate;
- lipsa armonizării legislative privind investigaţiile în domeniu;
- caracterul transnaţional al acestui tip de infracţiune;
-existenţa unui număr redus de tratate internaţionale privind extrădarea şi asistenţa mutuală în domeniu.

Elemente de prevenire a fraudelor informatice:

- **Implementarea şi dezvoltarea unui sistem eficace de control intern;**
- **Securizarea accesului la sistemele informaţionale;**
- **Asigurarea transparenţei tuturor activităţilor: Evaluarea procedurilor de achiziţii publice, a tranzacţiilor cu risc major de fraudă;**
- **Segregarea sarcinilor, consolidarea supravegherii activităţilor ce implică riscuri majore;**
- **Implementarea procedurilor de control utilizarea principiului „patru ochi";**
- **Stabilirea unei politici adecvate de recrutare;**
- **Managementul riscurilor de fraudă.**

Curmarea fraudelor informatice în RM:

Cadru legislativ

- **Legea nr. 20 din 03 februarie 2009 ”Privind preve--nirea şi combaterea criminalităţii informatice”- stabileşte funcţiile autorităţilor şi instituţiilor publice competente în domeniul prevenirii şi combaterii fraudelor informatice.**
- **Legea nr.91 din 27.06.2014 "privind semnătura electronică şi documentul electronic"-sporeşte nivelul de securitate a semnăturilor electronice.**
- **Directiva 2006/24/CE a Parlamentului European şi a Consiliului din 15 martie 2006- păstrează datele generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile.**
- **Directiva 2002/58/CE „Privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice”**

Concluzii

Un investigator în domeniul criminalităţii informatice poate lucra la maximum 3-4 cazuri pe lună, în timp ce un investigator tradiţional poate soluţiona între 40 şi 50 de cazuri în aceeaşi perioadă de timp.

Elaborarea tehnicilor şi metodologiilor de cercetare a infracţiunilor informatice. Datorită caracterului transfrontalier al fraudelor informatice, armonizarea legislaţiei cu cea internaţională trebuie să vizeze, în principal: dreptul de autor, confidenţialitatea datelor, prevenirea şi combaterea fraudelor informatice, precum şi promovarea standardelor tehnice care să asigure intercomunicarea noilor reţele de telecomunicaţii.

Republica Moldova se află în prima etapă de dezvoltare a ramurii respective şi întâmpină mari greutăţi în dezvoltarea de mai departe. Prin urmare, pentru a construi o societate informaţională sănătoasă, statul, în primul rând, trebuie să ia toate măsurile necesare pentru a asigura securitatea subiecţilor participanţi la relaţiile informaţionale.

Concluzii

- Orice atac nu este altceva decât o încercare de a folosi imperfecțiunea sistemului de securitate al victimei fie pentru a obține informații, fie pentru a dăuna sistemului, de aceea motivul oricărui atac de succes este profesionalismul hackerului și valoarea informațiilor, precum și competența insuficientă a administratorului sistemului de securitate, în special software-ul imperfecțiunii și atenția insuficientă la problemele de securitate din companie în principiu.

Sarcini de autoevaluare

- Prezentarea unei infortmații analitice privind prevenirea și curmarea fraudelor informatice;
- Determinați instrumentele şi metodele de luptă cu amenințările cibernetice;
- Evaluați motivele criminalității cibernetice;
- Descrieți eforturile întreprinse pentru asigurarea securităţii informațiilor şi de securitate națională, în general.

Teme pentru lucru individual

- Structuri de securitate într-o societate democratică
- Infracțiuni pe Internet: hârțuirea electronică
- Considerațiuni privind protecția drepturilor de proprietate intelectuala pe Internet
- Politica și strategia de stat în domeniul informațional în contextul Integrării Europene a Republicii Moldova
- Protecția și securitatea sistemelor informaționale.

BIBLIOGRAFIE

- **Oprea D. Protecția și securitatea sistemelor informaționale. Suport de curs, Iași, 2017.**
- **Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică. București 2004, 71 p.**
- **Legea nr. 286/2009 privind noul Cod Penal, publicată în Monitorul Oficial nr. 510 din 24 iulie 2009, în vigoare de la 1 februarie 2014.**
- **Înșelăciune prin sisteme informatice, fraudă informatică și fals informatic. Percheziții domiciliare http://www.juridice.ro/295789/diicot-inselaciune-prin-sisteme-informatice-frauda-informatic-si-fals-informatic-perchezitii-domiciliare.html**