Forme de manifestare a pericolelor în spațiul cibernetic. Infracțiuni informatice

1. Clasificarea amenințărilor

Amenințările la adresa securității se realizează prin exploatarea vulnerabilităților.

Vulnerabilitatea este o slăbiciune a unui activ sau a unui grup de active, care pot fi exploatate de către unul sau mai multe amenințări.

Managementul vulnerabilității este o funcție de bază pentru securitatea ITC.

Managmentul vulnerabilității este o practică ciclică de identificare, clasificare, remediere şi atenuare a vulnerabilităţilor.

Vulnerabilitatile din retea reprezinta AUR pentru hackeri/crackeri: ofera posibilitatea accesării resurselor aflate în rețea și pot da acces la informații confidențiale, la date personale, pot încălca drepturile de autor sau chiar bloca activitatea.

Sursa vulnerabilităților:

- configurarea neadecvată a sistemelor și echipamentelor;
- defecte software (bug-uri), erori de programare, software malițios;
- mod de organizare: utilizarea tehnologiilor învechite și neactualizate;
- mecanisme nesigure de control al accesului;
- instruire insuficientă a utilizatorilor și apariția greșelilor accidentale;
- amplasarea neprotejată a clădirilor, camerelor, server-elor, mediilor de comunicații.

Soluții de management al vulnerabilității sunt scanerele de rețea, web application scanning, vulnerability management, exploit kit-urile ale vendorilor de securitate:Qualys, McAfee, Saint, Acunetix etc.

Amenințările la adresa integrității, cofidențialității şi disponibilității sistemelor și serviciilor electronice și de comunicații se pot exercita prin mai mulţi vectori. Cei mai frecvenţi, sunt:

- utilizatorii răutăcioşi sau răuvoitori;
- anumite persoane din interiorul organizaţiei (insideri), care au acces la date şi procedeile utilizate în sistemul de securitate al organizaţiei respective;
- persoane din afara organizaţiei (autsideri)dar care au acces la anumite informaţii extrem de sensibile pentru securitatea organizaţiei;
- programele malitioase, spionii;
- organizaţiile criminale şi teroriste;
- cataclismele naturale.

O altă clasificare, presupune:

1) Amenințări de natură umană

- <u>acțiuni deliberate</u>
  acces neautorizat la date și sistem
  interceptare/modificare trafic
  denial of service
  cod/program malițios
  furt sau distrugere de date sau echipamente
  inginerie socială (social engineering)
- <u>accidente</u> – erori de operare

2) De natură tehnică

- **î**ntrerupere alimentare cu energie
- defectare echipamente

3) De mediu

- dezastre naturale
- condiții exterioare (contaminare, interferență electromagnetică)

Metoda STRIDE elaborată de Microsoft, este un acronim ce vine de la șase categorii de amenințări:

- ***S****poofing (falsificarea identității):* reprezintă pretinderea de a fi altcineva prin obținerea accesului ilegal asupra datelor;
- ***T****ampering (fraudarea datelor):* reprezintă procesul de modificare a datelor precum modificarea datelor dintr-o bază de date sau alterarea datelor aflate în tranzit;
- ***R****epudiation (repudierea):* repudierea este asociată cu utilizatorii care neagă efectuarea unei acțiuni fără ca celelalte părți să poate demonstra inversul; de exemplu, un utilizator a efectuat o operație ilegală într-un sistem care nu are un mecanism de urmărire a acțiunilor efectuate;

- ***I**nformation disclosure (dezvăluirea informației):* implică expunerea informațiilor sensibile individualilor care nu ar trebui să aibă acces la informațiile respective; de exemplu, abilitatea unui utilizator de a citi un fișier la care nu au acces;
- ***D**enial of service (întreruperea serviciilor):* reprezintă un atac care previne accesul legitim la resurse; de exemplu, făcînd un serviciu web temporar indisponibil;
- ***E**levation of privilege (ridicarea nivelului de privilegii):* reprezintă un atac în care un utilizator obține acces privilegiat și prin urmare are privilegii suficiente pentru a compromite sau a distruge întregul sistem; ridicarea nivelului de privilegii include situațiile în care un utilizator a trecut de toate mecanismele de securitate a sistemului, devenind parte de încredere a sistemului.

Ținta ameniță̆rilor:

- *Sistemele informatice și procesele care le execută* – instrucțiunile programelor și datele care sunt prelucrate de aceste programe;
- *Datele* – reprezentarea de fapte, concepte sau instrucțiuni, într-o modalitate potrivită pentru comunicare, interpretare sau procesare: dstele curente din memorie, fișiere stocate sau informații transmise prin mediul de comunicații;
- *Sistemul de calcul* - dispozitivele fizice care constau din una sau mai multe componente asociate, incluzând unități de procesare, de memorie și periferice, controlate de programele stocate intern;
- *Componenta* (fizică sau logică) sistemului de calcul sau a rețelei de comunicații;
- *Conturi de utilizator sau administrator* – domeniul de acces al utilizatorului (în sistem sau rețea), care este controlat conform unor înregistrări ce conțin numele contului, parola și drepturile de acces la cont;
- *Rețelele de comunicații și Internetul* – grupul interconectat de echipamente de rețea sau rețele interconectate.

2. Tipuri de ameniță̆ri

Acces neautorizat la date și sistem (Acces ilegal)

Pentru obţinerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi atacul: prin parolă; de acces liber; care exploatează slăbiciunile tehnologice; care exploatează bibliotecile partajate; IP; prin deturnarea TCP etc.

Spargerea parolelor. Procesul de ghicire a parolelor poate fi automatizat prin utilizarea unui program care ghiceşte parolele în permanenţă, cunoscut sub numele de tehnică de spargere a parolelor prin *forţă brută* (brute force password-cracking technique). Un program care execută asemenea atacuri este disponibil pe scară largă în Internet. Programul de atac prin forţă brută va încerca parole gen aa, ab, ac etc., până când a încercat fiecare combinaţie posibilă de caractere. În final, hackerul va obţine parola.

Atacul parolelor prin dicţionar. În general, aceste programe simple rulează pe rând fiecare cuvânt din dicţionar, în încercarea de a găsi o parolă. Astfel, atacurile prin parole automate au devenit rapid cunoscute sub denumirea de atacuri cu dicţionarul (dictionary-based attacks).

RISCURI ȘI RECOMANDĂRI

Cele mai bune soluţii împotriva atacurilor prin dicţionar sunt: modificarea sistematică a parolelor, rularea periodică a unui program de analiză a sistemului pentru verificarea parolelor.

Un tip interesant de acces ilegal, din ce în ce mai utilizat astăzi, îl reprezintă atacurile prin *inginerie socială*. Acestea au devenit mai frecvente şi mai periculoase. Un exemplu frecvent de inginerie socială este ca un hacker să trimită mesaje email către utilizatori (sau pur şi simplu să folosească telefonul) pentru a-i anunţa pe aceştia că el este administratorul sistemului. Deseori, mesajele solicită utilizatorilor să-şi trimită parola prin email către administrator, fiindcă sistemul este într-o pană sau va fi dezafectat temporar.

Un atac prin inginerie socială se bazează cel mai mult pe ignoranţa utilizatorilor în materie de calculatoare şi reţele.

RISCURI ȘI RECOMANDĂRI

Cea mai bună rețetă împotriva ingineriei sociale o reprezintă educaţia utilizatorilor.

Interceptarea ilegală a unei transmisii de date informatice

Interceptarea pachetelor - spionaj în reţea (network snooping) sau supraveghere ascunsă (promiscous monitoring), reprezintă una dintre infracţiunile cele mai dificil de realizat, şi este, de asemenea, o ameninţare serioasă la adresa comunicaţiilor prin Internet.

Fiecare pachet trimis prin Internet poate tranzita un număr mare de calculatoare şi reţele înainte de a ajunge la destinaţie. Prin intermediul unui *interceptor de pachete* (sniffere), hackerii pot intercepta pachetele de date (inclusiv cele cu mesaje de login, transmisii ale identificatorilor numerici ai cărţilor de credit, pachete email etc.) care călătoresc între diferite locaţii din Internet. După ce interceptează un pachet, hackerul îl poate deschide şi poate fura numele hostului, al utilizatorului, precum şi parola asociată pachetului.

RISCURI ŞI RECOMANDĂRI

Pentru a preveni atacurile de interceptare ilegală asupra reţelelor se recomandă să fie folosite schemele de identificare, cum ar fi un sistem cu parolă unică (OTM) sau un sistem de autentificare prin tichete (Kerberos). Criptarea datelor transmise la fel prezintă o soluție eficientă de protecție.

În general, sniffer-ele sunt utilizate de administratorii de reţea sau de Internet Service Provideri (ISP) pentru realizarea analizei de trafic în cadrul unei reţele în scop tehnic, de mentenanţă. Totodată, acestea sunt folosite de către administratorii reţelelor unor instituţii pentru monitorizarea comunicaţiilor (interne sau externe) ale angajaţilor.

De exemplu, sistemul *Carnivore* dezvoltat de către Biroul Federal de Investigaţii al SUA (FBI), menit să faciliteze agenţiei accesul la activităţile informatice desfăşurate de potenţialii infractori. Un alt sistem creat, la fel, de FBI a fost *Omnivore*, utilizat, în special, pentru supravegherea traficului de mesaje de poştă electronică. Alt sistem, mult mai complex, poate fi menționat *DragonWare Suite*.

O altă metodă de interceptare indirectă sau de la distanţă o constituie folosirea programelor tip keylogger, adware, spyware.

Programele de tip *Adware* şi *Spyware* se încarcă automat în PC-ul personal în momentul vizitării unei anumite pagini Web. Scopul lor este de a înregistra "traseul online" şi a transmite înapoi celor care le-au trimis (de obicei este vorba despre companii care fac comerţ prin Internet, firme de marketing şi publicitate) date şi informaţii despre preferinţele utilizatorului în materie de pagini Web, conţinut, tematică etc.

Un program *Keylogger* este o aplicaţie specializată care înregistrează fiecare tastă pe care o apasă un utilizator şi trimite informaţiile către persoana care a instalat programul. Acest software poate extrage informaţii extrem de folositoare, cum ar fi numărul cărţii de credit, rapoarte ale companiei, informaţii secrete dintr-o instituţie sau date cu caracter financiar. Tot în aceeaşi gamă există şi programele de monitorizare a emailurilor: *Websense, MIMEsweeper, FastTrack etc*.

RISCURI ŞI RECOMANDĂRI

Pentru a ajuta la protejarea computerului de programe spion, utilizați un program antispyware, (de exemplu, WindowsDefender).

Banala tastatură. În esenţă, se pot decoda sunetele produse de butoanele tastaturii. Cercetătorii de la Berkley, Universitatea California, au descoperit că o simplă înregistrare a sunetelor produse de tastatură poate fi folosită pentru descifrarea textului scris de utilizator, indiferent dacă este o parolă, o scrisoare de dragoste sau un secret de stat. Experţii în computere ai renumitei instituţii academice au înregistrat timp de 10 minute sunetele produse de o tastatură. Fişierul audio rezultat a fost introdus într-un computer şi "decriptat" cu ajutorul unui software special. Au fost recuperate cu exactitate 96% din caracterele scrise de utilizator. Asta înseamnă că textul a putut fi dedus fără nici o problemă, chiar dacă mai lipsea câte o literă la câteva cuvinte.

Astăzi persoane interesate captează, cu ajutorul unor dispozitive speciale, radiaţiile electromagnetice existente în imediata vecinătate a monitorului computerului ţintă, pe care le „traduc" transformându-le în impulsuri electrice şi, mai apoi, în caractere alfanumerice.

RISCURI ŞI RECOMANDĂRI

Tehnologia de protecţie a sistemelor de calcul împotriva captării emisiilor se numeşte TEMPEST – Transient ElectroMagnetic Pulse Emanation STandardizing.

Alterarea integrităţii datelor informatice

Cele mai periculoase instrumente care alterează datele informatice sunt însă programele tip Virus, Vierme sau Cal Troian, care se reproduc şi se pun în lucru în alte programe ori fişiere de date ca programe de distrugere.

Virusul de calculatoare este unul dintre cele mai comune riscuri la adresa securităţii reţelelor. Ca şi un virus medical, un virus de calculator se extinde prin ataşarea la programe sănătoase (echivalentul celulelor sănătoase). După infectarea unui sistem, virusul de calculator se ataşează de fiecare fişier executabil, fişier obiect sau ambele, situate în sistemul unde se află virusul. Mai mult, unii viruşi infectează sectorul de boot al unităţilor de disc.

Există mai multe clase de viruşi. Fiecare clasă foloseşte o metodă diferită pentru a se reproduce. Printre cele mai frecvente şi interesante tipuri de viruşi amintim: viruşii de criptare polimorfici şi nonpolimorfici, viruşii invizibili, viruşii lenţi, viruşii retro, viruşii multipartiţi, viruşii protejaţi şi viruşii fagi, viruşii macro etc.

Virusul Cal Troian se ascunde în codul unui fişier non-executabil (de exemplu, fişiere comprimate sau fişiere document) sau, în unele cazuri, chiar într-un fişier executabil pentru a nu fi detectat de majoritatea programelor antivirus. Un Cal Troian va intra în execuţie după ce a trecut cu bine de programul de detecţie antivirus. Deseori, viruşii Cal Troian apar sub masca unor programe utile sau ca fişiere bibliotecă în cadrul unui fişier arhivă comprimat.

Viermele Internet produce căderea unui sistem prin crearea unui număr extrem de mare de copii ale acestuia în memoria calculatorului, eliminând toate programele din memorie. Deoarece un virus-vierme are tendinţa să dezactiveze calculatorul infectat, hackerii construiesc în general viruşi-viermi care trec de la calculatorul infectat la un altul, aflat în conexiune cu primul. Viruşii-viermi se copiază pe alte calculatoare folosind protocoale obişnuite.

RISCURI ŞI RECOMANDĂRI

O soluţie este de a memora informaţia şi programele de securitate pe medii izolate, nemodificabile, cum ar fi o unitate WORM – unitate de stocare pe suport optic.

Perturbarea funcţionării sistemelor informatice

Un astfel de exemplu este *Denial of Service* - DOS (refuzarea serviciului) în care o resursă de pe Internet, cum ar fi un server sau un site Web nu mai funcţionează corespunzător deoarece atacatorii lansează un atac coordonat care supraîncarcă ţinta cu atât de multe solicitări false, încât sistemul nu mai poate să le administreze şi este copleşit.

Cel mai comun tip de atac DoS are ca efect împiedicarea accesului utilizatorilor de Internet la un anumit site Web, ceea ce poate avea ca rezultat pierderi financiare imense în contextul unei organizaţii ale cărei afaceri depind de Internet.

O altă modalitate prin care un atacator poate să preia controlul asupra unui sistem informatic sau să introducă aplicaţii maliţioase este prin intermediul *Codului Mobil*. Acesta este o categorie de cod scris (in limbajele Java, JavaScript şi ActiveX) şi încadrat într-un document tip HTML. Când browser-ul utilizatorului încarcă pagina de Web, codul mobil ascuns este descărcat şi executat de către browser.

Operaţiuni ilegale cu dispozitive sau programe informatice

Un exemplu în acest sens poate fi conceperea, cu ajutorul limbajului de programare de nivel înalt C++, a unui program care, pus în execuţie pe un computer, permite accesul unei persoane neautorizate la resursele sale ori la întregul sistem informatic la care este conectat, prin efectuarea unei operaţiuni de „identificare” a parolei ori codului de acces. Cele mai periculoase programe informatice sunt Backdoors, RootKit.

Backdoors (ușile din spate) permit ca un dipozitiv al unei rețele să fie controlat de alt dspozitiv de la distanță, printr-un utilitar de administrare a retelelor.

Rootkit-ul face referire la acel cod software utilizat pentru modificarea sau simularea funcţiilor de bază ale unui sistem de operare, dând posibilitatea unui atacator să acceseze un sistem informatic de la distanţă. Un rootkit poate, de exemplu, să fie disimulat în comanda dir (windows) sau ls (unix), astfel încât pe lângă funcţia de bază a acelei comenzi să realizeze şi alte acţiuni despre care utilizatorul nu este conştient .

Rootkit sunt împărţite în două categorii:

- *user – mode*: modifică cod software din sistemul de operare folosit la nivel utilizator (dir, ch, ls);
- *kernel – mode*: modifică cod software din sistemul de operare utilizat la nivel nucleu (kernel) - servicii, daemons, procese şi fire de execuţie, management întreruperi etc.

Falsul informatic

Poate lua una din următoarele forme:

- Simularea poştei electronice;
- Simularea hyperconexiunilor;
- Simularea Web-ului.

Frauda informatică

Frauda poate fi comisă cu ajutorul mai multor mijloace: poştă electronică, telefon, cablu, Internet etc. În mediul informatic, frauda poate avea mai multe forme şi adesea se poate confunda cu înşelăciunea tradiţională, mijlocul de realizare fiind computerul. Dat fiind mediul informatic în care acestea sunt iniţiate şi derulate:

- Bait and switch (momeşte şi schimbă);
- Scrisorile nigeriene;
- Prizonierul spaniol;
- Facturarea falsă;
- Înfiinţarea de firme „fantomă”.

Programele malițioase răspândite la moment sunt de tip *Ransomware,* ce împiedică accesul la fișiere, sau chiar la întregul sistem informatic infectat, până la plata unei „recompense" (ransom). Este una dintre cele mai supărătoare forme de malware, întrucât produce pagube financiare directe, iar de cele mai multe ori fișierele criptate de malware nu pot fi decriptate. Pentru a îngreuna procesul de recuperare a fișierelor, ransomware-urile blochează accesul la fișiere (documente, fotografii, muzică, video etc.) prin criptarea asimetrică a acestora. Cele mai recente versiuni sunt *Wanna Cry*, care a afectat companii și instituții din aproape 200 de țări (mai 2017) și ***Petya/Petrwrap*, care se răspândește doar în reteaua internă unde a avut loc infecția inițială a unei stații de lucru,** realizată prin intermediul unor documente atașate unor mesaje email de tip phishing, pe care utilizatorii sunt îndemnati să le deschidă (iunie 2017).

RISCURI ȘI RECOMANDĂRI

1. Majoritatea atacurilor vizează exploatarea componentei umane (social engineering, phishing, spear phishing, spam etc.). În consecință, nu accesați link-urile sau atașamentele conținute de mesajele email suspecte înainte de a verifica, în prealabil, sursa/legitimitatea acestora.
2. O atenție sporită trebuie acordată site-urilor web pe care le accesați și surselor online pe care le utilizați pentru descărcarea sau actualizarea aplicațiilor.
3. *Cea mai eficientă metodă pentru combaterea amenințării ransomware este realizarea periodică de backup (copii de rezervă)* pentru datele stocate/procesate cu ajutorul sistemelor informatice. **IMPORTANT!** Pentru backup utilizați un mediu de stocare extern care nu este conectat în permanență la sistem.
4. Activați opțiunile de tip *System Restore* în cazul sistemelor de operare Windows pentru toate partițiile de stocare. Datele ar putea fi rapid restaurate prin aducerea sistemului la o stare anterioară. **ATENȚIE!** Nu vă bazați exclusiv pe această facilitate deoarece unele versiuni recente de ransomware șterg datele din System Restore.

3. Infracțiuni informatice în reglementări internaționale

Convenţia Consiliului Europei asupra Criminalităţii Informatice, semnată la Budapesta la 23 noiembrie 2001, încearcă în principal să armonizeze dispoziţiile de drept substanţial cu caracter penal în domeniul informatic, să implementeze dispoziţii procedurale necesare pentru investigarea şi urmărirea unor asemenea infracţiuni şi să pună la punct un sistem rapid şi eficient de cooperare internaţională.

Convenţia are, în consecinţă, patru capitole:

I – Înţelesul unor termeni şi expresii;

II – Măsuri necesare a fi luate la nivel naţional – Drept penal şi procedură penală;

III – Cooperarea internaţională;

IV – Dispoziţii finale.

Secţiunea I a cap. al II-lea (dispoziţii de drept penal) se referă atât la incriminarea unor fapte ca infracţiuni, cât şi la alte aspecte de drept material, referitoare la răspunderea penală, participaţie şi sancţiuni.

Sunt definite aici nouă infracţiuni grupate în patru categorii diferite. Astfel, sunt considerate infracţiuni aducând atingere confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice:

- *Accesarea ilegală* (art.2);
- *Interceptarea ilegală* (art.3);
- *Alterarea integrităţii datelor* (art.4);
- *Alterarea integrităţii sistemului* (art.5)
- *Abuzurile asupra dispozitivelor* (art.6).

Sunt prevăzute ca infracţiuni în legătură cu mediul informatic:

- *Falsificarea informatică* (art.7);
- *Frauda informatică* (art.8).

O altă categorie de infracţiuni se referă la:

- *Pornografia infantilă* (art.9)

Ultima categorie face referire la:

- *Infracţiuni care aduc atingere proprietăţii intelectuale şi drepturilor conexe* (art.10).

Secţiunea a II-a a cap. al II-lea se referă la dispoziţii procedurale în materie penală, aplicabile în cazul săvârşirii infracţiunilor prevăzute în secţiunea I, în cazul săvârşirii oricărei infracţiuni de drept comun prin intermediul sistemelor informatice, ori în situaţiile în care dovada săvârşirii oricărei infracţiuni se regăseşte stocată într-un sistem informatic.

Totodată, se stabilesc condiţiile şi măsurile de protecţie aplicabile în cazurile mai sus menţionate. Astfel, se instituie măsuri privind:

- conservarea rapidă a datelor informatice stocate (art.16);
- conservarea şi dezvăluirea parţială rapidă a datelor referitoare la trafic (art.17);
- ordinul de punere la dispoziţie a datelor (art.18);
- percheziţia şi sechestrarea datelor informatice stocate (art.19);

- colectarea în timp real a datelor referitoare la trafic (art.20);
- interceptarea datelor referitoare la conţinut (art.21).

De asemenea, sunt prevăzute dispoziţii referitoare la competenţă.

Capitolul al III-lea conţine dispoziţii privind asistenţa judiciară internaţională în materie penală în privinţa infracţiunilor săvârşite prin mijloace informatice, incluzând şi dispoziţii referitoare la extrădare. Sunt prevăzute astfel două situaţii privind asistenţa judiciară:

- când nu există nici o bază legală privind asistenţa judiciară între părţi, situaţie în care se aplică prevederile cap. al III-lea;
- în situaţia în care această bază legală există, iar în acest caz dispoziţiile cap. al III-lea vin numai să completeze dispoziţiile lacunare, dacă există.

Cooperarea judiciară se referă la dispoziţiile procedurale prevăzute în cap. al II-lea, secţiunea a II-a, dispoziţii enumerate mai sus. În plus, sunt prevăzute în acest capitol dispoziţii privind accesul direct de la un sistem informatic aflat pe teritoriul naţional la date stocate într-un sistem informatic aflat pe teritoriul unei alte ţări, în două situaţii, fără a fi nevoie de asistenţă judiciară, respectiv atunci când se obţine consimţământul persoanei care are dreptul să dispună de aceste date, ori în situaţia în care aceste date au fost puse anterior la dispoziţia publicului.

De asemenea se pun bazele unei reţele de cooperare care să funcţioneze non-stop între statele semnatare, pentru a prelua şi rezolva cu promptitudine cererile de asistenţă judiciară.

Capitolul al IV-lea conţine clauzele finale, care cu câteva excepţii, repetă dispoziţiile standard din tratatele Consiliului Europei. Republica Molodva a implementat în întregime dispoziţiile acesteia.

4. Infracțiuni informatice în reglementări naționale

Infracţiunile informatice se clasifică în:

- Infracțiuni săvârșite cu ajutorul sistemelor informatice, în care sistemele informatice constituie un instrument de facilitare a comiterii unor infracțiuni. Este vorba de infracțiuni *tradiționale,* perfecționate prin utilizarea sistemelor informatice.
- Infracțiuni săvârșite prin intermediul sistemelor informatice, în care sistemele informatice, incluzând și datele stocate în acestea, constituie ținta infracțiunii. Aceste infracțiuni pot fi săvârșite doar prin intermediul sistemelor informatice.

Infracțiuni săvârşite cu ajutorul sistemelor informatice:

- Infracțiunea de reproducere, fără drept, a unei opere, reglementată de art.20, 23 din Legea privind dreptul de autor și drepturilor conexe, nr.293-XIII din 23.11.1994.
- Infracțiunea de reproducere, fără drept, a programelor pentru computer, reglementată de art. 23 din Legea privind dreptul de autor și drepturilor conexe, nr.293-XIII din 23.11.1994.
- Infracțiunea de spălare a banilor din Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, nr.633-XV din 15.11.2001.
- Infracțiunea de trădare prin transmitere de secrete, reglementată de art.337 din Codul penal.
- Infracțiunea de divulgare a secretului care periclitează siguranța statului, reglementată de art.344 din Codul penal.
- Infracțiunea de propagandă, reglementată de art.140 din Codul penal.

Infracțiuni săvârşite prin intermediul sistemelor informatice:

- Accesul ilegal la un sistem informatic. Infracțiunea de acces fără drept la un sistem informatic este prevăzută în art.259 din Codul penal: *Accesul ilegal la informația computerizată.*
- Introducerea sau răspândirea programelor virusulente. Infracțiuni de cest gen sunt prevăzute în art.260 din Codul penal: *Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program* (art. 260^1 Interceptarea ilegală a unei transmisii de date informatice; art. 260^2 Alterarea integrităţii datelor informatice ţinute într-un sistem informatic; art. 260^3 Perturbarea funcţionării sistemului informatic; art. 260^4 Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare; art. 260^5 Falsul informatic; art. 260^6 Frauda informatică)
- Încălcarea regurilor de securitate la diferite sisteme informatice. Astfel de infracțiuni sunt reglementate de art.261 din Codul penal: *Încălcarea regulilor de securitate a sistemului informatic* (art. 261^1 Accesul neautorizat la reţelele şi serviciile de telecomunicaţii).
- Pornografia infantilă. Infracțiuni de cest gen sunt prevăzute în art. 208. din Codul penal: *Atragerea minorilor la activitate criminală sau determinarea lor la săvîrşirea unor fapte imorale* (art. 208^1. Pornografia infantilă).

5. Etapele de investigare a infracțiunilor informatice

Legislația Republicii Moldova a înputernicit mai multe organe speciale cu atribuții de relevare a atentatelor criminale, de prevenire, curmare, descoperire a infracțiunilor și a persoanelor care le organizează, le comit sau le-au comis, *inclusiv a infracțiunilor informaționale și a fraudelor prin Internet*. Astfel:

1. Conform art.266 CPP, competența organului de urmărire penală a MAI care efectuează urmărirea penală pentru orice infracțiune care nu este dată prin lege în competența altor organe de urmărire penală sau este dată în competența lui prin ordonanța procurorului.

2. Conform art.269 CPP, competența organului de urmărire penală al CCCEC care efectuează urmărirea penală în privința infracțiunlor prevăzute la art. 236-261[1], 324-326, 330-336 din Codul penal.

3. Conform art.273 CPP, sunt abilitate cu funcții de control și alte servicii de stat care participă nemijlocit la verificarea activității economico-financiare a întreprinderilor, instituțiilor, organizațiilor de stat și a organelor administrației publice locale și centrale.

4. Conform HG RM cu privire la aprobarea Regulamentului Agenției Naționale pentru Reglementare în Telecomunicații și Informatică, nr.843 din 18.08.2000, toate aceste organe sunt abilitate cu atribuții de depistare a infracțiunilor, inclusiv a infracțiunilor informaționale și a fraudelor prin Internet, însă doar serviciile operative ale MAI, SIS, SV și CCCEC, în calitate de organe de constatare, sunt împuternicite atât cu funcții de depistare, cât și cu funcții de verificare a faptelor prejudecabile, în volumul deplin până la pornirea urmăririi penale, iar organele MAI și ale CCCEC exercită și urmărirea penală.

5.1. Probatoriul

Probatoriul se realizează după următoarele direcții de bază:

- acumularea de date care confirmă faptul comiterii unor acțiuni ilegale cu utilizarea informației electronice și a tehnicii de calcul;
- efectuarea acțiunilor de urmărire penală și a altor măsuri de stabilire a legăturii cauzale dintre acțiunile care constituie metoda de efectuare a unei operații nelgitime și survenirea urmăririlor prin detalierea caracterului acțiunilor comise de către persoana vinovată;
- stabilirea mărimii pagubei cauzate de acțiunile ilegale;
- acumularea și fixarea faptelor care confirmă implicarea persoanei bănuite sau învinuite de comiterea acțiunilor și survenirea rezultatelor.

Sosind la locul percheziției sau al examinării, este necesar:

- să se între imediat și inopinat în încăperea unde se află calculatorul, pentru a reduce la minimum posibilitățile de distrugere a informației care se află în calculator;

RISCURI ȘI RECOMANDĂRI

În unele cazuri, înainte de a intra în încăperea unde urnează a fi efectuată percheziția, aceasta să fie deconectată de la rețeaua de alimentare cu curent electric.

Personalul să fie trecut în altă încăpere.

RESTRICȚII

De a interzice tuturor persoanelor care lucrează la calculatoare din obiectivul la care se efectuează percheziția, precum și altor persoane, să se atingă de calculatoarele care funcționează, de mediile de stocare a informațiilor, de tastele de conectare/deconectare a calculatoarelor.

De a interzice întregului personal să conecteze sau să deconecteze alimentarea cu energie electrică a obiectivului.

În procesul de examinare a sistemului de calcul aflat în stare de funcționare este necesar:

- a se determina în ce program se lucrează în acel moment. Pentru aceasta, se va studia imaginea de pe ecranul monitorului, care va fi reflectată detaliat în procesul-verbal. În caz de necesitate, se fotografiază sau se înscriu pe video imaginile privind ecranul monitorului;
- a opri executarea programului, cu reflectarea în procesul-verbal a rezultatelor acţiunilor întreprinse de către persoana care efectuează examinarea; se vor indica, de asemenea, schimbările care au avut loc pe ecranul monitorului;
- a se stabili prezenţa instalaţiilor exterioare ale calculatorului de acumulare a informaţiei pe discuri magnetice (HDD/SSD), pe discuri şi instalaţii tip ZZP, prezenţa discului virtual (disc temporar care se formează la pornirea calculatorului pentru accelerarea funcţionării sale). Toate datele obţinute se vor include în procesul-verbal;
- a se stabili prezenţa instalaţiilor exterioare de acces de la distanţă la sistem şi a se determina starea lor (conectarea la reţeaua locală, prezenţa modemului), după care calculatorul şi modemul vor fi deconectate de la reţea, reflectînd în procesul-verbal rezultatele acţiunilor effectuate;
- a se copia programele şi fişierele cu datele create pe discul virtual (dacă acesta există) pe un suport magnetic sau pe discul de bază staţionar într-un director aparte;
- a deconecta calculatorul şi *a* continua examinarea calculatorului care nu se află în stare de funcţionare.

În procesul examinării este necesar:

- a indica în procesul-verbal şi în schema anexată la el locul aflării calculatorului şi a instalaţiilor sale periferice (printerul, modemul, tastatura, monitorul etc.), destinaţia fiecăreia din ele, denumirea, numărul de serie, completarea

(prezenţa şi tipul instalaţiilor pentru discuri, cartelă de reţea, grupa de contante etc.), prezenţa conexiunii cu reţeaua locală de calculatoare sau cu reţelele de telecomunicaţii, starea instalaţiilor (întreagâ sau cu urme de desfacere);

- a descrie exact ordinea de interconectare a instalaţiilor indicate, marcînd (în caz de necesitate) conductoarele de conexiune şi locurile de conexiune, după care instalaţiile calculatorului vor fi deconectate;
- a se stabili, cu ajutorul unui specialist, prezenţa în interiorul calculatorului a unor piese străine, sustragerea unor microscheme, deconectarea sursei interne de alimentare cu curent electric (acumulatorului);
- a se împacheta (cu indicarea în procesul-verbal a locului depistării lor) suporturile magnetice, optice etc. Pentru împachetare se pot utiliza atît casete speciale de păstrare, cît şi pachete de hîrtie sau polietilenă, care exclud nimerirea prafului, a murdăriei pe suprafaţa de lucru a discului;
- a se împacheta fiecare componentă a calculatorului şi conductoarele de conexiune. Pentru excluderea accesului altor programe, vor fi sigilate blocul, butonul de conectare a calculatorului şi locul de conectare a conductorului electric, de asemenea, locurile de unire a părţilor laterale cu panourile din faţă şi din spate ale calculatorului.

5.2. Numirea expertizei

Expertiza este activitatea de cercetare efectuată de către un specialist, denumit expert, avînd ca obiectiv stabilirea adevărului, a realităţii într-o anumită situaţie sau referitoare la un anumit eveniment.

Fiind un mijloc de constatare, confirmare, dovedire, lămurire a realităţii privind un eveniment, o faptă, o situaţie, pe baza cunoştinţelor de specialitate, expertiza este un mijloc de probă.

Pentru soluţionare în faţa expertizei tehnico-programiste se pot pune următoarel întrebări:

- Ce fel de informaţii conţin blocurile de sistem şi purtătorii magnetici? Care sînt destinaţia şi posibilităţile lor de utilizare?
- Ce fel de programe se conţin pe suporturile magnetice de stocare a informaţiei? Care sînt destinaţia şi posibilităţile lor de utilizare?
- Blocurile de sistem şi suporturile magnetice conţin şi fişiere textuale? Dacă da, atunci care este conţinutul şi posibilităţile lor de utilizare?
- Pe suporurile magnetice se află informaţie distrusă?
- Este posibilă restabilirea acesteia? Dacă da, atunci care este conţinutul şi posibilităţile sale de utilizare?
- Ce fel de produse de program se conţin pe suporturile magnetice? Care sînt conţinutul, destinaţia şi posibilităţile lor de utilizare?
- Pe suporturile magnetice se află programe specializate, utilizate pentru selectarea parolei sau a altui procedeu de pltrundere ilegală într-o reţea de calculatoare? Dacă da, atunci care sînt denumirile lor, particularităţile de acţiune, posibilităţile de utilizare pentru pătrunderea într-o anumită reţea computerizată?
- Există semne care să confirme utilizarea unui program anume pentru pătrunderea ilegală într-o anumită reţea computerizată? Dacă da, atunci care este structura cronologică a acţiunilor necesare pentru pornirea unui anumit program sau pentru executarea unei operaţiuni concrete?
- Lucrînd într-o anumită reţea computerizată, este posibilă efectuarea în produsele program a unor modificări ale fişierelor de program? Dacă da, atunci în ce mod şi de la ce calculator pot fi făcute schimbările respective?
- E posibil de a obţine acces la o informaţie confidenţială care se află într-o anumită reţea? În ce mod se efectuează un astfel de acces?
- În ce mod are loc un accesul ilegal într-o reţea computerizată locală?
- Care sînt semnele ce confîrmă o astfel de pătrundere?
- Dacă un acces ilegal a avut loc din afară, atunci care sînt posibilităţile de identificare a calculatorului de la care a avut loc acest acces?
- Dacă nu există semne de pătrundere într-o reţea de calculatoare de la un utilizator extern, atunci cum se poate constata de la ce calculator este posibilă efectuarea unei operaţiuni asemănătoare?

La soluţionarea expertizei pot fi formulate întrebări privind compatibilitatea unor programe, posibilitatea utilizării unui anumit program la un anume calculator şi altele în afară de aceasta, se pot pune întrebări privind destinaţia unui sau altui obiect utilizat în tehnica de calcul

- Care este destinaţia şi posibilităţile de utilizare ale acestui obiect? Ce fel de particularităţi de construcţie are acesta?
- Din ce părţi constă acesta? A fost elaborat în condiţii industriale, casnice sau artizanale?
- Dacă obiectul respectiv a fost confecţionat în condiţii artizanale, atunci din ce domeniu al ştiinţei, tehnicii sau meşteşugăritului este persoana care a creat acest obiect şi care este nivelul său de professionalism?
- Împreună cu ce obiecte și aparate ar putea fi utilizat obiectul menţionat?

5.3. Investigații informatice

Investigarea criminalistică a sistemelor informatice prezintă o serie de particularităţi care o diferenţiază în mod fundamental de alte tipuri de investigaţii. Investigarea criminalistică a sistemelor informatice poate fi definită ca: *Utilizarea de metode ştiinţifice şi certe de asigurare, strîngere, validare, identificare, analiză, interpretare, documentare şi prezentare*

a probelor de natură digitală obţinute din surse de natură informatică în scopul facilitării descoperirli adevărului în cadrul procesului penal.

Un posibil model de bune practici în domeniul investigaţiilor criminalistice de natură informatică cuprinde următorii paşi:

1. Identlficarea incidentului - recunoaşterea unui incident şi determinarea tipului acestuia. Nu reprezintă efectiv o etapă a investigaţiei criminalistice, dar are un impact semnificativ asupra următoarelor etape.

2. Pregătirea investigaţiei - pregătirea instrumentelor, verificarea procedurilor, obţinerea documentelor ce permit percheziţia etc.

3. Formularea strategiei de abordare - formularea unei strategii în funcţie de tehnologia implicată şi de posibilele consecinţe asupra persoanelor şi instituţiilor impiicate. Scopul formulării acestei strategii este să maximizeze potenţialul obţinerii de probe relevante, minimizînd, în acelaşi timp, impactul negativ asupra victimei.

4. Asigurarea probelor - izolarea, asigurarea şi păstrarea probelor de natură fizică şi digitală. Aceasta include îndepărtarea celora care ar putea denatura probele în orice fel.

5. Strîngerea probelor - înregistrarea ambianţei fizice şi copierea probelor digitale folosind practici şi proceduri comune şi acceptate.

6. Examinarea probelor – examinarea în profunzime a probelor, căutarea elementelor care sînt în legătură cu fapta penală investigată. Acest lucru presupune localizarea şi identificarea probelor, precum şi documentarea fiecărui pas, în scopul facilitării analizei.

7. Analiza probelor - determinarea semnificaţiei probelorşi relevarea concluziilor cu privire la fapta investigată.

8. Prezentarea probelor - sintetizarea concluziilor şi prezentarea lor într-un mod inteligibil pentru nespecialişti. Această sinteză trebuie susţinută de o documentaţie tehnică detaliată.

9. Restiîuirea probelor - dacă este cazul, returnarea către proprietarii de drept a obiectelor reţinute în timpul investigaţiei. Dacă este cazul, determinarea, în funcţie de prevederile legilor procedurale penale, a confiscării obiectelor.

Următoarele crlterii sînt utile în aprecierea oportunităţii privind ridicarea sistemelor informatice:

- *Criteriul volumului probelor*. Particularitatea sistemelor informatice de a permite stocarea unui volum foarte mare de informaţie într-un spaţiu de dimensiuni fizice reduse face ca investigaţia să necesite un volum mare de timp pentru obţinerea probelor relevante. Astfel de cercetări pe o perioadă de timp mare pot fi conduse mult mai eficient în laborator.
- *Criteriul dificultăţilor de natură tehnică*.

Procedura ridicării sistemelor informatice poate fi divizată în următoarele etape:

1. Inchiderea sistemului. Dacă sistemul a fost găsit închis în momentul pătrunderii investigatorilor, acesta nu trebuie sub nici un motiv pornit. Se va proceda în continuare trecînd la celelalte etape. Dacă sistemul a fost găsit deschis, el trebuie închis, pentru a se putea proceda la ridicarea lui. Pentru închiderea sistemului se pot folosi următoarele procedee:

- deconectarea de la alimentarea cu energie electrică;
- închiderea conform procedurii normale.

2. Etichetarea componentelor. În cazul în care se impune dezasamblarea, fiecare componentă a sistemului trebuie etichetată înainte de modificarea configuraţiei în vederea ridicării probelor. În cazul cablurilor, se etichetează atît cablul, cît şi suporturile de unde a fost debranşat. în cazul existenţei unor suporturi care nu au conectate cabluri, este recomandabil ca să fie etichetate "neocupat". Se poate realiza şi o schiţă a componentelor, cu precizarea simbolurilor folosite pentru etichetare.

3. Protejarea la modificare. Toate suporturile magnetice de stocare a datelor trebuie protejate împotriva modificării conţinutului lor. Unele tipuri de hard-diskuri au contacte proprietăți speciale care realizează protejarea la scriere.

4. ***Ridicarea propriu-zisă.*** Ridicarea probelor trebuie făcută cu multă grijă, evitîndu-se orice avariere a componentelor. Este recomandabilă împachetarea componentelor în ambalajul original, dacă acesta poate fi găsit, sau în ambalaj special ce asigură protecţia electrostatică a acestora. De asemenea, toate suporturile magnetice de stocare a datelor vor fi ambalate şi sigilate în aşa fei încît accesul la ele să nu fie permis, pînă la desfacerea în laborator.

Copierea trebuie realizată după un procedeu demn de încredere. Pentru a putea avea această caracteristică, copierea trebuie:

- să asigure posibilitatea verificării de către terţi; instanţa de judecată sau partea adversă, să poată să verifice acurateţea copiei realizate;
- să aibă ca rezultat copii sigure, ce nu pot fi falsificate.

Bibliografie

1. Maxim Dobrinoiu, *Infracțiuni în domeniul informatic,* București, 2006.

2. Gheorghe Alecu, Alexei Barbăneagră, Regrementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic, Ed. Pinguin Book, 2006.
3. Gheorghe Alecu, Particularități ale investigației penale și criminalistice a unor infracțiuni din domeniul informatic, AP, 8/2, 2005.
4. Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică, USAID din România, Bucureşti, 2004.
5. Veaceslav Soltan, *Tehnologii informaționale,* Cartea XX, Institutul Național al Justiției, Chișinău, 2009.
6. Legea privind prevenirea şi combaterea criminalităţii informatice, nr. 20-XVI din 03.02.09.
7. Hotărârea Guvernului Nr. 811 din 29.10.2015 privind aprobarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020.
8. Hotărârea Guvernului Nr. 201 din 28.03.2017 privind aprobarea Cerinţelor minime obligatorii de securitate cibernetică.
9. Codul penal al R.M.