INFRACȚIUNILE INFORMATICE

Autor: Alexandru PAPUC, student TI-162

Universitatea Tehnică a Moldovei

Abstract: *Dezvoltarea calculatoarelor a avut, și are până în prezent un impact major asupra vieții de zi cu zi, asupra modului de desfășurare a afacerilor, de gestiune a informației e.t.c. Totodată dezvoltarea tehnologiilor au adus și la apariția noilor infracțiuni, cu caracter extrem de sofisticat, și anume infracțiunile informatice. Tipurile de asemenea infracțiuni sunt multiple, printre ele se enumeră frauda informatica, sabotajul informatic, falsul informatic e.t.c, pirateria software ocupând cea mai mare parte a acestor infracțiuni. Infractorii din domeniul dat, în special hackerii, folosesc soft-uri extrem de sofisticate, ce determină ca depistarea lor să fie practic imposibilă, iar atacurile lor să aducă prejudicii irecuperabile companiilor. Astfel rețelele informatice au ajuns să ocupe o lume aparte, în care infractorii sunt cei care o conduc, iar justiția, deocamdată, fiind departe de această lume.*

Cuvinte cheie: *piraterie software, fraudă informatică, sabotaj informatic, hacker, gruparea "Anonymous".*

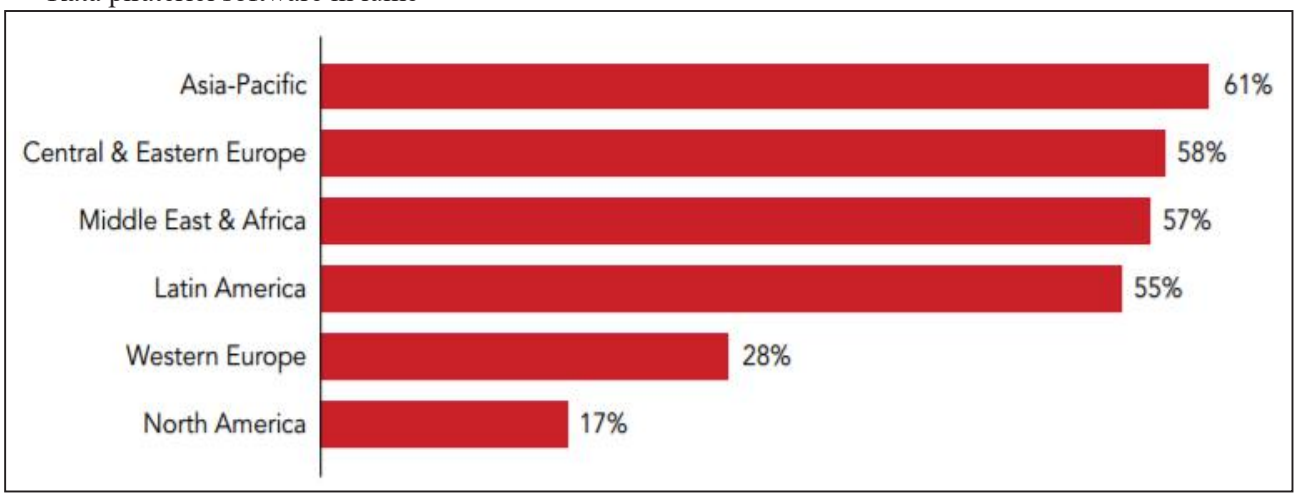
Ce este o infracțiune informatică?

Calculatoarele au pătruns în activităţile tuturor ţărilor, devenind instrumente indispensabile pentru desfăşurarea diferitelor activităţi. Acestea au avut un impact global asupra vieţii de zi cu zi, asupra modului de desfăşurare a afacerilor, de comunicare şi de gestiune a informaţiei. Totodată, această evoluţie rapidă şi radicală ridică o serie de probleme atât de ordin socio-economic, în privinţa temerilor referitoare la locurile de muncă, dar şi juridice, spre exemplu în privinţa protecţiei programelor pentru calculator. Astfel dezvoltarea tehnologiilor a deschis posibilitatea apariţiei unei game largi de acţiuni ilegale cu un caracter extrem de sofisticat, şi anume infracţiunile informatice. Infracțiunea informatică constituie orice abuz informatic, cu comportament ilegal, neautorizat, care privește tratarea automată a datelor și/sau o transmisie de date.

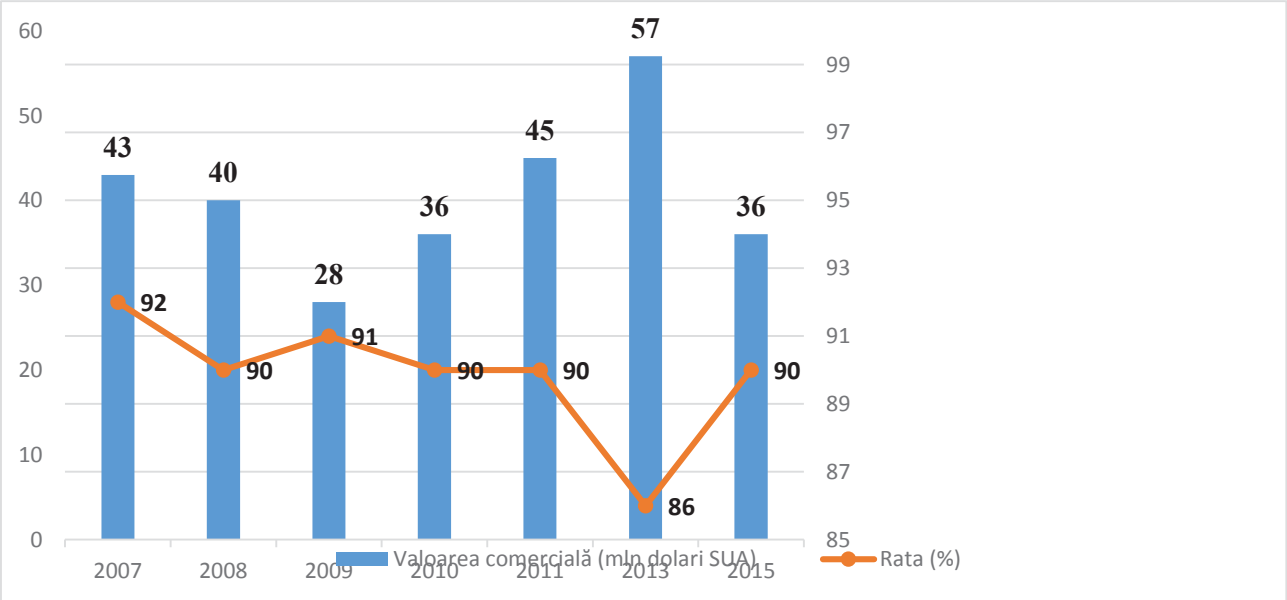
Unele tipuri de infracțiuni informatice:

Pirateria software. Investiţiile foarte mari făcute în competenţe şi experienţe, costurile mari de elaborare şi testare ale programelor pentru calculator care merită să fie protejate prin dreptul de proprietate intelectuală, pe de e o parte, și uşurința și cheltuielile minime cu care se pot copia aceste programe, pe de altă parte, constituie factorii care favorizează infracțiunile de acest gen. Statisticile arată că pirateria software reprezintă cea mai mare parte a crimelor informatice (85-90% din total).

Rata pirateriei software în lume[5]



Rata pirateriei software și valoarea comercială a produselor nelicențiate în Republica Moldova[5]



Trebuie de menţionat faptul că spionajul informatic este orientat în mare parte anume pe programele piratate, utilizatorul unor astfel de atacuri fiind mai vulnerabil contra altor infracţiuni informatice. Se pedepseşte conform art.260 Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program[4]:

- cu o amendă în mărime de la 500 la 1000 unităţi convenţionale
- sau cu închisoare de la 2 la 5 ani
- sau cu amendă, aplicată persoanei juridice, în mărime de la 3000 la 6000 unităţi convenţionale, cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

La fel pedepsită este şi utilizarea unor astfel de softuri, şi anume conform art.185.1 Încălcarea drepturilor de autor şi a drepturilor conexe[4]:

- cu amendă în mărime de la 800 la 4000 de unităţi convenţionale
- sau cu muncă neremunerată în folosul comunităţii de la 180 la 240 de ore,
- iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 6000 de unităţi convenţionale

cu privarea de dreptul de a exercita o anumită activitate pe un termen de la 1 la 5 ani.

Frauda informatică. Activele înmagazinate şi administrate utilizând sistemele informatice - ca de exemplu fondurile electronice , depozitele , gestiunea stocurilor şi conturilor, ghişeele automate - au devenit ţinta manipulărilor de proprietate, la fel ca şi în cazul formelor clasice. Frauda informatică, este o infracţiune cu un grad de periculozitate înalt şi este caracterizată de fapte precum introducerea, modificarea, ştergerea sau restricţionarea accesului la aceste date sau programe, sau orice altă intervenţie care poate cauza un prejudiciu material sau economic intenţionat, infractorul urmărind scopul obţinerii unui avantaj financiar. În practica juridică s-a ajuns la concluzia că aceste infracţiuni sunt greu de identificat şi imposibil de urmărit din cauza numeroaselor lacune ale dreptului penal clasic, dar şi a noilor mijloace tehnice ce determină depistarea lor să fie practic imposibilă. Se pedepseşte conform art. 260.6 Frauda informatică[4]:

- cu amendă în mărime de la 1000 la 1500 unităţi convenţionale
- sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore,
- sau cu închisoare de la 2 la 5 ani.

În cazuri mai grave, precum cauzarea daunelor în proporţii deosebit de mari se pedepseşte cu închisoare de la 4 la 9 ani.

Interceptarea ilegală a unei transmisii de date informatice. Datorită mijloacelor tehnice actuale a devenit posibilă punerea sub ascultare şi supraveghere a sistemelor de transmisie de date la distanţă, interceptarea de date în curs de transmisie sau pornind de la emisii electronice, cum ar fi, de exemplu, terminalele. Această faptă constă în interceptarea ilegală a unei transmisii de date informatice (inclusiv a unei emisii electronice) care nu sânt publice şi care sânt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic. Se pedepseşte conform art.260.1 Interceptarea ilegală a unei transmisii de date informatice[4]:

- cu amendă în mărime de la 500 la 1000 unităţi convenţionale
- sau cu închisoare de la 2 la 5 ani,

- cu amendă, aplicată persoanei juridice, în mărime de la 3000 la 6000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

Falsul informatic. Majoritatea legislațiilor penale naționale în materie de fals prevăd ca afirmațiile sau declarațiile care figurează într-un document să poată fi descifrate cu ochiul liber, astfel ele nu se aplică datelor informatice, creând serioase lacune. Falsul informatic constituie introducerea, modificarea sau ștergerea ilegală a datelor informatice ori restricționarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice. Se pedepsește conform art. 260.5 Falsul informatic[4]:

- cu amendă în mărime de la 1000 la 1500 unități convenționale
- sau cu închisoare de la 2 la 5 ani

Sabotajul informatic. Perturbarea funcționării sistemelor informatice și ale celor de telecomunicații pot avea consecințe mult mai nefaste decât alterarea datelor sau a programelor pentru calculator. Prin sabotaj informatic se înțelege perturbarea funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date. Se pedepseşte conform art. 260.3 Perturbarea funcționării unui sistem informatic [4]:

- cu amendă în mărime de la 700 la 1000 unităţi convenţionale
- sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore,
- sau cu închisoare de la 2 la 5 ani, cu amendă

În unele cazuri, cum ar fi săvârşirea infracţiunii în grup, pedeapsa poate fi mai mare:

- amendă în mărime de la 700 la 1000 unităţi convenţionale
- sau închisoare de la 3 la 7 ani

Cine sunt infractorii ?

Subiecţii care atentează la securitatea informaţiei pot aparţine unor categorii diverse, comițând delicte mai mult sau mai puţin grave, în linii generale putând fi clasificate în persoane din interiorul unei organizaţii şi incidentele şi persoane din exterior – care reprezintă o sursă majoră de risc din considerentele că sânt mai dificil de depistat şi investigat decât cele din interiorul organizaţiilor. Pentru o abordare mai specifică aceste două categorii majore de infractori, după specificul activităţii lor şi modul de utilizare a informaţiei, pot fi divizate în segmente mai mici precum ar fi angajaţi, consultanţi sau personal de întreţinere a sistemului, furnizori sau clienţi, competitori, hackeri sau infractorii profesionişti, experţii în spionaj, accidente sau dezastre naturale.

O categorie ce prezintă un interes aparte este cea a persoanelor din exterior şi anume a hackerilor. Hackerii sunt pasionaţi ai informaticii, care, de obicei au ca scop „spargerea" anumitor coduri, baze de date, pagini web etc. La rândul lor hackerii se împart în amatori și profesioniști.

Hackerii amatori sunt cei care atacă ţinte aleatoare, oriunde şi oricând au ocazia. În marea lor majoritate acţiunile lor au un caracter distractiv. De exemplu, atacurile tot mai frecvente asupra Yahoo şi Hotmail au blocat motoarele de căutare şi conturile de mail respective pentru câteva zile, aducând prejudicii de milioane de dolari. Aceşti hackeri amatori sunt singurii care ajung în faţa justiţiei. Motivul este simplu. Acei hackeri adevăraţi care îşi pot scrie singuri programele, sunt, de obicei destul de inteligenţi pentru a face anumite sisteme care să inducă în eroare pe toţi aceea care ar încerca să determine sursa atacului.

Hackerii profesioniști sunt cei care au cunoștințe vaste în domeniu, experiență, de obicei lucrează în grup. Ţintele lor obişnuite sunt sistemele importante, care au protecţii avansate şi conţin informaţii strict secrete, cum ar fi bazele de date ale Pentagonului sau cele de la NASA. Odată obţinute, aceste fişiere (informaţii) sunt publicate pe tot Internet-ul, pentru a fi vizionate sau folosite de cât mai multe persoane. Orice hacker adevărat trebuie să respecte un „Cod de legi al hackerilor", care este bine stabilit, cunoscut şi respectat.

Unul dintre cele mai cunoscute grupuri de hackeri este „Anonymous". Membrii acestei grupări pot fi recunoscuți după masca lui Gay Fawkes.

Emblema „*Anonymous*" și „*Anonymous*" în spațiu public, Los Angeles 2008

Printre acțiunile lor se numără numeroase spargeri de site-uri, deseori îndreptate împotriva instituțiilor de stat, ba chiar și împotriva Vaticanului. Ultima operațiune de amploare a fost spargerea și publicarea a 5000 de conturi ale membrilor grupării teroriste Statul Islamic, ca răspuns la atentatele din Paris din noiembrie 2015.

Crackerii. Un tip deosebit îl constituie crackerii, ei reprezintă un stil anumit de hacker, care sunt specializaţi în „spargerea" programelor shareware, sau care necesită un anumit cod serial. Singurii care sunt prejudiciaţi de această categorie de hackeri sunt cei care scriu şi proiectează programele „sparte". Sistemele de protecţie ale aplicaţiilor respective pot fi „înfrânte" prin două metode:

- Introducerea codului, care poate fi găsit fie pe Internet, fie cu ajutorul unui program asemănător cu OSCAR 2000, care este o bibliotecă de coduri.
- A doua metodă este folosită pentru sistemele de protecţie mai avansate, care necesită chei hardware (care se instalează pe porturile paralele ale computerului şi trimit un semnal codat de câte ori le este cerut de către programul software), sunt patch-urile. Ele sunt programele care sunt făcut special pentru anumite aplicaţii software, care odată lansate modifică codul executabil, inhibând instrucţiunile care cer cheia hardware.

Patch-urile şi bibliotecile de coduri seriale se găsesc cel mai des pe Internet. Ele sunt făcute de anumite persoane (care sunt câteodată foşti angajaţi ai firmelor care au scris software-ul respectiv) care vor doar să aducă pagube firmei proiectante. Totuşi, foarte rar sunt depistaţi cei care plasează patch-uri şi coduri seriale pe Internet.

Concluzii

Revoluţia tehnologiei informaţiei a dat naştere la schimbări economice şi sociale fără precedent, dar în acelaşi timp foloseşte şi scopurilor mai puţin legitime: apariția unor noi infracţiuni, ori săvârşirea infracţiunilor tradiţionale prin intermediul noii tehnologii. Conceptele juridice existente sunt puse la încercare de apariţia noii tehnologii. Adesea locul săvârşirii infracţiunii diferă de locul unde se găseşte infractorul. Printr-o simplă apăsare a unui buton acesta poate declanşa catastrofe la mii de kilometri depărtare. Aceste infracţiuni lezează patrimoniul organizaţiilor, instituţiilor, dar şi a persoanelor fizice. Reglementarea legală urmăreşte să protejeze sistemele informatice şi datele stocate pe acestea, de accesul neautorizat.

Bibliografie:

1. T.Amza, C.Amza „*Criminalitatea informatică*", Bucureşti 2003
2. Petre Rău „*Infracţionalitatea pe calculator*", Galaţi 2001
3. Pagini web cu infracțiuni informatice
4. Codul penal al Republicii Moldova
5. BSA Global software survey