Cristina VOINU, UCCM

INFRACȚIUNILE INFORMAȚIONALE ŞI MIJLOACE DE COMBATERE A LOR

Abstract: *The informational offences can challenge important destruction taking in consideration that is used by the user.The Republic of Moldova is not ready to fight with these offenders.In order to avaid these riskc it must be added a law about the informational affences.*

Revoluția tehnologiei informației a dus la schimbări fundamentale în societate şi este probabil ca aceste schimbări profunde să se producă în continuare.

Unul din efectele progresului tehnologic este impactul asupra evoluției telecomunicațiilor. Comunicarea clasică prin intermediul telefoniei a fost depăşită de noile metode de transmitere la distanţă nu numai a vocii, ci şi a datelor, muzicii, fotografiilor sau filmelor. Aceste schimburi de informații nu mai apar numai între oameni, dar şi între oameni şi sisteme informatice.

Folosirea poştei electronice sau accesul la paginile web prin intermediul Internetului constituie exemple ale acestei evoluții, modificând profund societatea noastră. Uşurința accesului la informație în sistemele informatice, combinată cu posibilitatea practic nelimitată de schimb sau disiminare a acestora, indiferent de granițele geografice sau naționale, a dus la o creştere explozivă a cantității de informație disponibilă şi a cunoştințelor ce pot fi extrase din aceasta.

Această evoluție a dat naştere la schimbări economice şi sociale fără precedent, dar în acelaşi timp foloseşte şi scopuri mai puțin legitime: apariția unor noi infracțiuni sau săvârşirea infracțiunilor tradiționale prin intermediul noilor tehnologii. Adesea locul săvârşirii infracțiunii diferă de locul unde se găseşte infractorul. Prin o simplă apăsare a unui buton acesta poate declanşa catastrofe la mii de km depărtare.

Conform legislației române, infracțiunea informațională reprezintă interceptarea fără drept a unei transmisii de date informatice, care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic.

A. Cel mai simplu atac hacker – atacul TCP/IP cu predicția numărului de secvențe foloseşte modalitatea de adresare a calculatoarelor în rețea şi schimburile de pachete pentru a obține acces într-o rețea.

B. Atacurile active prin desincronizare – o conexiune TCP impune un schimb sincronizat de pachete, dacă numerele de secvență ale pachetelor nu s/t cele aşteptate de către calculatorul receptor acesta va refuza pachetul şi va aştepta pachetul cu numărul corect. Pentru a ataca un sistem folosind atacurile prin desincronizare, hackerul induce sau forțează ambele extremități ale unei conexiuni TCP într-o stare desincronizată astfel, încât aceste sisteme să nu efectueze

schimbul de date. Apoi hackerul foloseşte un host terț pentru a intercepta pachetele reale şi pentru a crea pachete de înlocuire acceptabile.

C. Determinarea prin postsincronizare – să presupunem că hackerul poate asculta orice pachet schimbat între 2 sisteme care formează o conexiune TCP; să presupunem că după interceptarea fiecărui pachet, hackerul poate falsifica orice tip de pachet IP. Pachetul falsificat al hackerului îi permite să se dea drept client sau server.

D. Furtuna TCP ACK – în cazul unui atac TCP activ, primul pachet TCP ACK include propriul număr de secvență al serverului. Calculatorul-client nu va accepta acest pachet de conformare. Clientul îşi generează propriul pachet de confirmare care determină serverul să genereze un alt pachet de confirmare, creând ceea ce se numeşte un ciclu infinit pentru fiecare pachet de date transmise. Deoarece pachetele de confirmare nu transportă date, emițatorul pachetului ACK nu le retransmite pachetul dacă receptorul îl pierde. Dacă un sistem pierde un pachet în ciclul de furtună ACK, ciclul se încheie.

E. Sistemul CARNIVORE – un program controversat dezvoltat de către Biroul Federal de Investigații (FBI), menit să faciliteze agenției accesul la activitățile informatice desfăşurate de potențialii infractori. Carnivore a reprezentat cea de a 3-a generație de programe şi aplicații de supraveghere electronice folosite de FBI. A 2-a generație de programe de interceptare şi monitorizare IT a fost OMNIVORE – creat în special pentru supravegherea traficului de mesaje pe poşta electronica ce ajungea printr-un anumit internet servis provider şi captarea acestora în funcție de emitent.

F. Banala tastatura-aliata spionilor – 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. Experții în computere au înregistrat timp de 10 minute sunetele produse de tastatură. Fişierul audio rezultat a fost introdus într-un computer şi decriptat cu ajutorul unui software special. Au fost recuperate cu exactiatea – 96 % din caracterele scrise de utilizator.

G. Securitatea radiațiilor – toate echipamentele care funcționează pe bază de energie electrică produc energie electrică, emisă prin semnale electromagnetice necontrolabile, transmisibile prin aer, ca undele radio, sau de-a lungul firelor sau materialelor conductibile, ca orice curent electric. Astfel de radiații de la calculatoare sau de la cablurile de comunicații pot fi purtătoare de informații, ce pot fi extrase de către persoane interesate din afară, după o analiză mai specială.

Protecția echipamentelor de prelucrare automată a datelor utilizate pentru informațiile speciale împotriva riscului generat de propriile lor radiații este una dintre cele mai dificile probleme puse în fața agențiilor specializate.

Există un număr substanțial de măsuri, relativ ieftine, de diminuare a pericolului răspândirii datelor prin intermediul radiațiilor necontrolate. Dintre ele amintim:

a) zonele sterile – se recomandă crearea unor zone sterile în jurul echipamentelor de prelucrare automată a datelor, prin îndepărtarea tuturor corpurilor metalice din apropierea lor;

b) telefoanele – în timp ce datele se afişează pe ecran, telefonul, chiar dacă este în repaus, poate transmite date oriunde în afara organizației, de aceea nu trebuie plasat lângă monitoare;

c) curenții filtranți – radiațiile necontrolate pot fi diminuate prin transmiterea în cablu a unor curenți filtranți;

d) accesul – controlul accesului în organizație al persoanelor sau al prezenței vehiculelor în apropierea centrului de prelucrare a datelor;

e) amplasarea echipamentelor în birouri – se evită plasarea echipamentelor de calcul lângă ferestre, se vor plasa toate componentele fizice în centrul sălii sau clădirii;

f) echipamentele moderne – seturile actuale de echipamente electronice de calcul tind să dea mai puține radiații decât vechile modele.

g) curățirea ecranelor – ştergerea ecranului după ce nu mai e nevoie de datele afişate şi nu se recomandă listarea de probă de prea multe ori a documentelor ce conțin date secrete;

h) derutarea – în jurul pieselor de bază ale centrului de prelucrare automată a datelor se plasează unele echipamente care să prelucreze date lipsite de importantă, dar care vor fi interceptate de inamicii sistemului.

Făptuitorii acestor tipuri de infracțiuni pot fi grupați în mai multe categorii. Într-o categorie s-ar plasa: hackerii, spionii, teroriştii, atacatorii, criminalii de profesie şi vandalii. Din altă categorie fac parte: novicele, ucenicul, vizitatorul, amatorul şi profesionistul. Toți aceşti infractori folosesc informația în scopuri diferite.

În Republica Moldova, de asemenea, apare tendința creşterii infracțiunilor săvârşite cu ajutorul computerului. Protecția de drept de infracțiuni de acest tip, practic, nu există în legislația R.Moldova. Nu există calificarea infracțiunilor săvârşite cu ajutorul computerului şi nu este stabilită ordinea de profilactică şi descoperire a asemenea infracțiuni.

Culegerea ilegală sau răspândirea cu bună-ştiință a informațiilor, ocrotite de lege, se pedepseşte cu amendă în mărime de până la 300 de unități convenționale sau cu munca neremunerată în folosul comunității de la 180 la 240 de ore. Răspândirea informațiilor: a) într-un discurs public, prin mass-media; b) prin folosirea intenționată a situației de serviciu – se pedepseşte cu amendă în mărime de la 200 la 500 de unități convenționale sau cu arest de până la

6 luni. Codul penal impută responsabilitate pentru violarea dreptului la secretul corespondenței (art.178) şi accesul ilegal la informația computerizată (art.259). Conform legislației, persoana vătămată prin răspândirea unei informații se va apăra invocând normele juridice privind protecția vieții private numai în cazul în care această informație este adevărată.

Bibliografie:

1. V.Patriciu. Criptarea şi securitatea rețelelor de calculatoare, Editura Tehnică, Bucureşti, 1994, p.22.
2. L.Klander. Anti-hacker, Editura All Educational, Bucureşti,1998, p.248.
3. L.Bird. Internet-Ghid complet de utilizare, Editura Corint, Bucureşti, 2004, p.331.
4. R.Mihalca. Bazele dezvoltării produselor software, Editura ASE, Bucureşti, 2003, p.17;
5. Legea privind accesul la informație //Monitorul Oficial-2000, nr.88-90, 28 iulie.
6. Legea cu privire la informatică // Monitorul Oficial-2001, nr.73-74, 5 iulie.
7. Internet -http://www.efraude.ro/

   -http://moldova.cc/fraude/Detectarea%20Fraudelor.htm

   -http://www.berkley.edu