RISCURI DE ATAC ASUPRA SISTEMELOR INFORMAȚIONALE

Autor: Sinelnicov V.

Conducător ştiinţific: Maftei V. l.superior

Universitatea Tehnică a Moldovei

Abstract: *Informatizarea grabnică a societăţii a ajuns la nivel global şi utilizarea informaticii în rezolvarea problemelor, prin procedee care fac disponibile informaţiile este din ce în ce mai solicitată în toate sferele societăţii. Noua civilizaţie informatică se bazează pe disponibilitatea şi accesibilitatea informaţiei. Informaţia a devenit o proprietate vitală, cu o valoare strategică: dacă nu este protejată, poate fi cucerită sau distrusă. Este o axiomă faptul că societatea informaţiei bazată pe cunoaştere are un impact profund asupra sistemului economic, social, politic şi juridic. In mai puţin de o generaţie, revoluţia informaţională şi introducerea calculatoarelor în virtual fiecare aspect al societăţii a schimbat lumea.*

Cuvinte cheie: *Informaţie, securitate, risc, atac electronic, sistem informaţional, hacker.*

Societatea informaţională este societatea în care producerea şi consumul de informaţie este cel mai important tip de activitate, informaţia este recunoscută drept resursă principală, tehnologiile informaţiei şi comunicaţiilor sunt tehnologii de bază, iar mediul informaţional, împreună cu cel social şi cel ecologic – un mediu de existenţă a omului.

În mai puţin de o generaţie, introducerea calculatoarelor şi respectiv developarea lor rapidă a schimbat în mare parte modalităţile de circulaţie a informaţiilor. De asemenea uşurarea accesului la informaţii oferă utilizatorilor un control operaţional sporit ceea ce reduce cu mult timpul de prelucrare a datelor necesare.

Analog, odată cu dezvoltarea tehnologiilor şi facilitarea accesului la informaţie, se ivesc diverse aspecte negative în domeniul informaticii, apar noi tipuri de infracţiuni; de exemplu crearea şi distribuirea viruşilor informatici. La fel infracţiunile tradiţionale precum furtul, frauda, falsul pot fi comise prin intermediul ultimelor tehnologii.

Răspândirea relativ rapidă a calculatoarelor din ce în ce mai performante şi disponibile la preţuri din ce în ce mai accesibile; de asemenea şi dezvoltarea reţelei mondiale de internet oferă eventualilor atacatori posibilitatea să acţioneze negativ realizând atacuri rapide care pot avea consecinţe destul de serioase, iar probabilitatea de detectare a infractorilor electronici este mică. Atacurile cibernetice pot avea urmări la nivel personal, organizaţional sau chiar şi politic.

Introducerea calculatorului în mersul majorităţilor activităţi moderne este esenţial pentru a asigura buna manevrare a respectivelor activităţi. şi de aceea securizarea calculatoarelor este un factor foarte important care trebuie neapărat de menţinut în continuu la un nivel înalt.

Factori care pot fi consideraţi că au crescut riscurile de atac:

- Globalizarea crescândă;
- Dificultăţile de securizare inerente;
- Disponibilitatea de informaţii privind penetrarea fără autorizaţie a sistemelor de informaţii;
- Insuficienta conştientizare şi educare a utilizatorilor sistemelor de informaţii, şi atitudinile sau practicile care nu respectă procedurile de folosire;
- Reglementări legislative neclare şi anumite dificultăţi jurisdicţionale.

Este evident că afectarea informaţiilor va crea dificultăţi persoanei sau organizaţiei căreia ele aparţin; rezultă că materialele necesare efectuării unei activităţi au o anumită valoare.

Cei ce pot cauza probleme de securitate asupra sistemelor informaţionale sunt:

a) Angajaţii care au acces deplin la sistemul informaţional şi deci ei cunosc slăbiciunile sistemelor;

b) Furnizorii sau Clienţii. Motivele lor economice nu sunt în unele cazuri congruente cu cele ale organizaţiei şi, în unele situaţii, pot efectua anumite acţiuni care pot prezenta riscuri de securitate;

c) Consultanţii ori Personalul de întreţinere al sistemului: Aceste persoane au adresa de acces la zonele sensibile ale sistemului informaţional, ceea ce le permite efectuarea unor operaţiuni cu mare diversitate;

d) Crackerii/Mercenarii informatici/Infractorii profesionişti. Aceştia penetrează sistemele în mod intenţionat şi ilegal cu scopuri diferite.

e) Competitorii. Alte persoane sau organizaţii care au de câştigat de pe urma pierderilor organizaţiei din urma atacurilor sistemului de informaţii.

f) Experţii în spionaj. Aceste persoane sunt bine plătite, fiind specializate în obţinerea anumitor informaţii (în mod ilegal) care va favoriza alte organizaţii. Aceşti experţi sunt foarte rar detectaţi;

g) Accidentele/Dezastrele naturale. Acestea pot cauza pierderea unor informaţii importante sau indisponibilitatea acestora.

Atacatorii sistemelor informaţionale pot avea diferite motivaţii cum ar fi:

- Motivaţia socială. Atacatorii din această categorie încearcă să obţină un sentiment de superioritate sau de control, de acceptare faţă de alţi atacatori sau de integrare într-un anumit grup;
- Motivaţia tehnică. Atacatorii din această categorie încearcă să *învingă* sistemul, ca un fel de provocare intelectuală.
- Motivaţia politică. Atacatorii din această categorie încearcă să obţină atenţia politică, pentru a promova o anumită cauză;
- Motivaţia financiară. Atacatorii din această categorie încearcă să obţină un câştig personal (cum ar fi, spre exemplu, spionii, mercenarii informatici, diverse organizaţii sau chiar persoanele care se ocupă cu distribuirea de informaţii confidenţiale etc.).

Protecţia calculatorului vostru împotriva viruşilor si hackerilor se poate face folosind câteva mijloace de apărare, cum ar fi firewall-ul, antivirusul, anti-spyware-ul, setarea corectă a browser-ului sau folosirea unor parole puternice.

Iată câteva masuri pe care trebuie sa le luaţi pentru a evita sa deveniţi o victima a viruşilor, hackerilor sau a viruşilor spies (spioni).

Instalaţi un firewall

Hackerii acţionează pe Internet la fel cum unii agenţi de marketing apelează automat numere oarecare de telefon. Ei trimit apeluri pentru mii de calculatoare si aşteaptă răspunsuri.
Firewall-ul împiedica calculatorul sa răspundă. Unele computere au setat firewall-ul pe poziţia "off". Asiguraţi-va ca firewall-ul este configurat corect si actualizat periodic. Folosiţi opţiunea online "Help" din calculatorul vostru pentru instrucţiuni.

Utilizaţi un software antivirus

Antivirusul scanează calculatorul si e-mail-urile voastre pentru găsirea viruşilor, apoi ii şterge. ţineţi-l in continuu activ si folosiţi automat opţiunea update a antivirusului, pentru a contracara ultimele vulnerabilităţi de securitate. Setaţi-l pentru a verifica zilnic existenta viruşilor.

Evitaţi spyware

Unii viruşi spyware înregistrează fiecare tasta pe care o apeşi, inclusiv parole si informaţii financiare. Semne prin care calculatorul vostru poate fi infectat: o serie brusca de ferestre pop-up, performanta scăzută a calculatorului si deschiderea nedorita a unor site-uri pe care voi nu le accesaţi.
Protecţia spyware este inclusa in anumite software-uri antivirus sau pot fi achiziţionate separat programe anti-spyware. Pentru a evita aceasta: descărcaţi software gratuit numai după site-urile de încredere. Nu daţi click pe linkurile cu ferestre pop-up sau pe spamurile primite pe e-mail.

Setaţi-vă browser-ul

Puneţi setările de securitate ale browser-ului pe opţiunea "Medium-high" sau "High". Pentru asta duceţi-va in secţiunea "Tools" a browser-ului vostru, apoi intraţi de opţiunea "Internet options". In "Security" setaţi opţiunile medium sau high. Actualizaţi-va sistemul si browser-ul in mod regulat, profitând de actualizările de securitate automate.

Folosiţi o parolă puternică

Alegeţi parole care sunt greu de ghicit. Folosiţi cel puţin opt caractere, cu o combinaţie de litere, numere si caractere speciale. Nu utilizaţi cuvinte uşor de găsit într-un dicţionar.

Securizaţi-vă reţeaua wireless

Daca utilizaţi o reţea wireless la domiciliu, alegeţi un router cu criptare. Când folosiţi o reţea publica

de Wi-Fi, evitați accesarea sau trimiterea de informații personale sensibile. Cumpărați o cartela de banda larga pentru telefonia mobila si conectați-o la computer, laptop sau telefon si folosiți accesul la Internet.

Fiți atent când faceți sharing

Schimbul de fișiere digitale (muzica, filme, fotografii) va poate expune la riscuri. S-ar putea descărcă un virus sau un spyware, care va face calculatorul vulnerabil in fata hackerilor.

Faceți cumpărături on-line in siguranță

Verificați site-urile de cumpărături înainte de a introduce numărul cardului vostru sau alte informații personale. Citiți politica de confidențialitate a site-ului respectiv si uitați-va daca exista opțiuni pentru schimbul de informații.

Tehnologiile de securitate a informației au mai multe componente şi atribute care trebuie considerate când se analizează riscul potențial.

Acestea pot fi clasificate în trei mari categorii :

1) *Confidențialitatea* - protecția informațiilor în sistem astfel încât persoane neautorizate nu le pot accesa. Este vorba despre controlarea dreptului de a citi informațiile. Aproape fiecare organizația are informații care, dacă sunt divulgate sau furate, ar putea avea un impact semnificativ asupra avantajului competițional , valorii de piață sau a veniturilor. Adițional, o organizație poate fi făcută responsabilă pentru divulgarea de informații private. Aspecte cruciale ale confidențialității sunt identificarea şi autentificarea utilizatorilor.

2) *Integritatea* - protecția informațiilor împotriva modificărilor intenționate sau accidentale neautorizate; condiția ca informația din sau produsă într-un mediu informatic reflectă sursa sau procesele pe care le reprezintă. Este vorba despre nevoia de a asigura ca informația şi programele sunt modificate numi în maniera specificată şi autorizată şi ca datele prezentate sunt originale, nealterate sau şterse în tranzit. Ca şi în cazul confidențialității, identificarea şi autentificarea utilizatorilor sunt elemente cheie ale unei politici de integritatea a informațiilor.

3) *Disponibilitatea* – se referă la asigurarea ca sistemele de calcul sunt accesibile utilizatorilor autorizați când şi unde aceştia au nevoie şi în forma necesară (condiția ca informația stocată electronic este unde trebuie să fie, când trebuie să fie acolo şi în forma necesară).

Bibliografie:

1. http://www.securitatea-informatica.ro/securitatea-informatica/riscurile-de-atac-asupra-securitatii-sistemelor-informationale/
2. http://www.ziare.com/internet-si-tehnologie/calculator/cele-mai-bune-metode-de-protectie-impotriva-virusilor-si-a-hackerilor-1078189
3. http://ro.wikipedia.org/wiki/Societate_informațională
4. http://www.egov.md/index.php/ro/centrul/newsletter/497-dezvoltarea-retelei-mondiale
5. https://docs.google.com/open?id=1L9MXSyCB7Ba23zDKrg6ftF0GCjeS5b46aH43kWlHxTuq7kI2I80-RKbvZ0Ep