Concepte legate de securitate

1.1. Amenințări legate de date

1.1.1. Diferențierea termenilor date și informații

- **Datele** sunt fapte brute, neorganizate, care trebuie să fie procesate. Datele pot fi simple, inutile, aparent aleatorii până când sunt organizate.
- **Informaţiile** sunt date procesate, care au sens în contextul în care sunt prezentate

1.1.2. Cybercrime

- Calculatorul şi internetul au devenit tehnologii uzuale, la fel ca şi televizorul şi telefonul. Aceste tehnologii fac parte din viaţa noastră, fapt ce a dus la vulnerabilitatea in faţa „crimelor" cibernetice.
- **Cybercrime** cuprinde orice activitate ilegală sau act criminal care se ocupă cu calculatoare şi reţele. În plus, cybercrime include, de asemenea, crime tradiţionale efectuate prin Internet, ca de exemplu:
  - crime de ură (hatecrime),
  - telemarketing,
  - fraudă pe internet,
  - furtul de Identitate şi al datelor cardului de credit. Furturile sunt considerate a fi crime cibernetice atunci când acestea sunt comise prin utilizarea unui computer şi internet.

1.1.3. Înţelegerea diferenţei dintre hacking, cracking şi ethical hacking

- Din cauza mediului jurnalistic, conceptul de **hacking** a devenit un termen negativ, în momentul actual acesta fiind descris ca procesul de ”spargere” a securităţii unui calculator sau a unei reţele, fără acordul proprietarului, în scopul manipulării datelor şi programelor din respectivul calculator sau utilizării resurselor computerului, însă, cei mai vechi programatori şi ingineri IT pretind că procesul de hacking înseamnă, de fapt, crearea unei tehnologii IT sau soluţionarea unei probleme prin intermediul calculatorului.
- Aceaştia susţin că procesul de „invadare" sau „spargere" a securităţii unui calculator sau a unei reţele se numeşte **cracking,** astfel că persoana ce realizează acest lucru se numeşte **cracker.** Există două tipuri de cracking:
  - Password cracking - „spargerea" parolelor aferente anumitor fişiere, fie manual (prin ghicirea parolei), fie automat (prin utilizarea unei aplicaţii software)
  - Software cracking - dezactivarea sau eliminarea unor caracteristici nedorite ale unei aplicaţii software (protecţia împotriva copierii, controlul datelor, numărul serial, cheia produsului etc).
- Când o companie doreşte să lanseze un program software pe piaţă, este nevoie să realizeze teste de securitate pentru a oferi o aplicaţie sigură, în special dacă aceasta implică stocarea unor informaţii confidenţiale sau plăţi bancare. Aceste teste constau în angajarea unor experţi IT pentru a testa securitatea aplicaţiei, practic aceştia fiind plătiţi să găsească modalităţi de a trece de sistemele de securitate ale aplicaţiei. Procesul menţionat se numeşte **ethical hacking,** aceasta însemnând că are un scop etic, nu fraudulos.

1.1.4. Recunoaşterea ameninţărilor legate de date, cauzate de forţă majoră, precum incendii, inundaţii, război, cutremure

- Fiecare persoană încearcă să îşi protejeze datele din calculator împotriva atacurilor electronice (hacking, cracking) sau împotriva viruşilor, însă puţine persoane iau în considerare şi „atacurile de forţă majoră" cum ar fi incendii, inundaţii, cutremure etc.
- Pentru **evitarea pierderii datelor** este necesar să se realizeze **copii de siguranţă (backup)** ale fişierelor din computer **pe un dispozitiv extern de stocare** (hard disk extern, CD, DVD, memorie USB). Se recomandă ca aceste copii să fie păstrate într-o **locaţie externă**, diferită de cea în care se află calculatorul ce conţine datele iniţiale protejată de incendii şi inundaţii şi **securizată împotriva accesului neautorizat**.
- O altă opţiune de backup al datelor, cu o dezvoltare şi utilizare din ce în ce mai mare, constă în utilizarea **seviciilor online de stocare**. Aceasta înseamnă copierea fişierelor pe servere din Internet ce aparțin Google Drive unor firme care oferă contra cost sau gratis astfel de servicii, cum ar fi **Skydrive, Google Drive, iCloud** etc. în acest fel se asigură accesul sigur la fişiere de la computere aflate în diferite locaţii, cu condiţia **existenţei unei conexiuni Internet**.

1.1.5. Recunoaşterea ameninţărilor legate de date cauzate de salariaţi, furnizorii de servicii şi persoane fizice externe

- **Angajaţii** - conform ultimelor sondaje, principala cauză a problemelor informatice cu care se confruntă firmele româneşti sunt chiar angajaţii acestora.
- 0 altă cauză ar fi şi slaba configurare a sistemelor IT. Cum însă şi acest lucru ţine tot de comportamentul angajaţilor, mai precis al celor specializaţi în securitate şi administrarea sistemelor IT, rezultă că majoritatea ameninţărilor la adresa unei companii vin chiar din partea celor care ar trebui să asigure protecţia informațiilor confidențiale ale acesteia.
- Angajaţii nu sunt neaparat rău intenţionaţi, ci pur şi simplu nu cunosc regulile elementare de securitate informatică, nefiind instruiţi în acest domeniu. De exemplu, angajații nu ştiu că nu trebuie să divulge parola de logare pe computer sau să o lase la vedere pe un bileţel. Un alt pericol constă în comportamentul anjagaţilor pe Internet, aceștia neavând cunoştinţe legate de securitatea online. O mare parte a atacurilor spyware are loc datorită faptului că angajaţii nu sunt atenţi atunci când introduc parolele conturilor de e-mail, când instalează diverse programe sau când accesează programe de mesagerie instantanee. De asemenea, angajaţii ar putea fura date importante și confidenţiale ale companiei pe care ulterior le pot dezvălui, voit sau nu unor persoane rău intenţionate.
- Rezultatele obţinute în urma sondajelor efectuate relevă faptul că, dacă firmele românești ar acorda training specializat angajaţilor cu privire la comportamentul adecvat în utilizarea calculatorului sau dacă ar folosi sisteme de monitorizare a activității acestora, aproape 60% dintre problemele legate de sistemele Informatice ar dispărea cu consecințe economice benefice pentru firmele care îşi instruiesc angajații
- **Furnizorii de servicii** - au acces la informaţii importante şi confidenţiale ale companiei. Ca urmare, aceştia trebuie să acorde o atenţie deosebită protejării acestor date confidenţiale întrucât riscă să îşi piardă clienţii dacă se produce o breşă în securitatea informaţiilor.
- **Persoane fizice externe** - pot obţine acces la un computer şi pot fura/şterge date. Aceste persoane se numesc cracker-i şi în general sunt plătiţi pentru a sparge parolele calculatoarelor şi a afla informaţii confidenţiale.