Concepte legate de securitate

1.2. Valoarea informației

1.2.1. Înţelegerea motivelor de protejare a datelor personale

- Pentru mulţi, un sistem de calcul este un „nod" de documente importante, fişieie şi aplicaţii, dar există întotdeauna un risc de a pierde sau compromite fişierele importante din cauza ameninţărilor exterioare.
- Ameninţările din afară au devenit o preocupare importantă pentru toţi utilizatorii, mai ales pentru cei care utilizează Internetul în mod regulat. Pornind de la programe maliţioase (viruşi şi viermi de calculator, programe spion şi înregistratori de taste), până la metode de însuşire a datelor personale (information diving, skimming, pretexting, phishing), pot cauza deteriorarea sistemului şi coruperea documentelor, dar mai ales infracțiuni cibernetice ca **furtul de identitate**. Acesta se prezintă ca un fenomen foarte grav, întrucât datele personale însuşite de persoane neautorizate pot fi folosite în activități ilegale sau frauduloase.
- Pentru **protejarea datelor** de ameninţări se recomandă următoarele:
  - Instalarea, **rularea** şi actualizarea regulată a aplicaţiilor antivirus.
  - **folosirea programelor** firewall.
  - Utilizarea **ultimelor versiuni** ale navigatoarelor (browsere) web şi **actualizarea** sistemului de **operare.**
  - Să se manifeste maximă prudenţă la e-mailurile şi telefoanele **care** solicită date personale și informaţii despre conturile bancare.
  - Să nu se deschidă ataşamente ale mesajelor provenite de la expeditori necunoscuți sau care nu prezintă încredere
  - Realizarea în mod regulat a copiilor de siguraţă (backup) ale documentelor importante

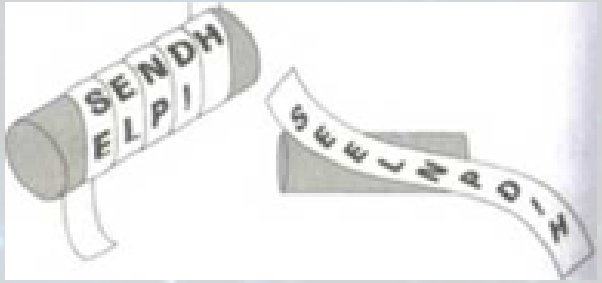
1.2.1. Înţelegerea motivelor de protejare a informaţiilor comerciale

- În prezent, resursele informaţionale au o importanţă majoră şi trebuie protejate. Fiecare organizaţie deţine secrete comerciale, ce includ informaţii cu privire la detaliile activităţii comerciale, relaţiile de afaceri, achiziţionarea materiei prime şi bunurilor, stabilitatea financiară a societăţii, metodologia de stabilire a preţurilor etc. Într-un mediu competitiv, protecţia informaţiilor confidenţiale reprezintă o problemă esenţială pentru că informaţiile referitoare la secretele comerciale pot fi folosite de alte persoane cu scopul de a provoca daune materiale şi morale.
- Măsurile care pot fi întreprinse pentru a asigura securitatea informaţiilor depind de natura şi domeniul de activitate al întreprinderii. Informaţiile pot fi protejate prin utilizarea măsurilor de ordin administrativ, juridic, organizatoric şi tehnic. De asemenea, cel mai eficient mod de protejare a datelor este aplicarea sistemică a acestor măsuri de securitate.
- De asemenea, există companii care folosesc colectori de date pentru a realiza diverse studii de piaţă înainte de a lansa un produs sau un serviciu. Aceştia au o serie de obligaţii legale, create pentru a preveni furtul şi abuzul datelor clienţilor:
  - Colectarea datelor în scopuri determinate, explicite şi legitime
  - Colectarea datelor adecvate, pertinente şi neexcesive prin raportare la scopul pentru care sunt colectate şi ulterior prelucrate
  - Stocarea datelor în condiţii de siguranţă, într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate
  - Prelucrarea cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare a datelor cu caracter personal.
  - Nedezvăluirea acestor informaţii persoanelor neautorizate.

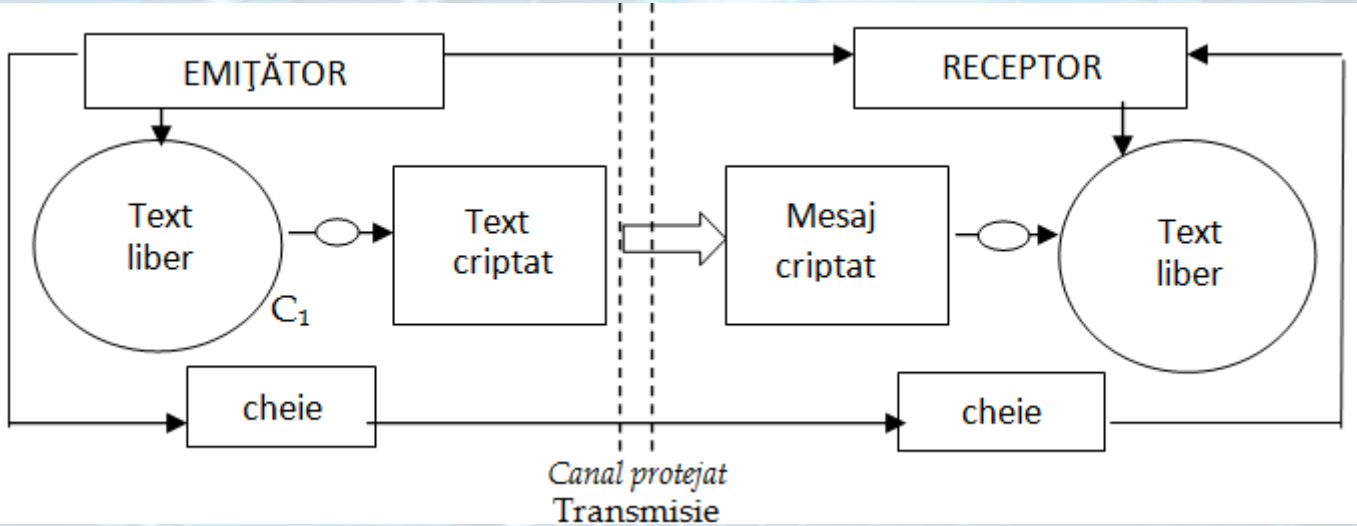
1.2.2. Identificarea măsurilor de prevenire a accesului neautorizat la date, precum criptare, parolare

- Când folosim Internetul, nu apăsăm doar click ca să luăm informaţii, cum ar fi citirea unor articole de știri sau posturi pe blog. O mare parte a timpului nostru online presupune trimiterea Informaţiilor noastre unor terţe persoane, respectiv calculatoare și dispozitive electronice.
- O comandă online a unui produs sau serviciu efectuată într-un magazin on-line sau accesarea unui cont de utilizator pe site-ul unei bănci sau de poştă electonică, necesită trimiterea de informaţii personale sensibile.
- O tranzacţie tipică ar putea include nu numai numele noastru, adresa de e-mail sau numărul de telefon, dar, de asemenea, parolele şi numerele personale de Identificare (PIN).
- Să recunoaştem, există o mulţime de informaţii pe care nu doriţi ca alte persoane să le vadă, cum ar fi:
  - Detalii personale (nume, prenume, CNP, număr de telefon ş.a).
  - Identificatori, nume de utilizatori şi parole pentru conturi de autentificare.
  - Detaliile cardurilor de credit/debit şi ale conturilor bancare.
  - Corespondenţa privată.
  - Documente confidenţiale.

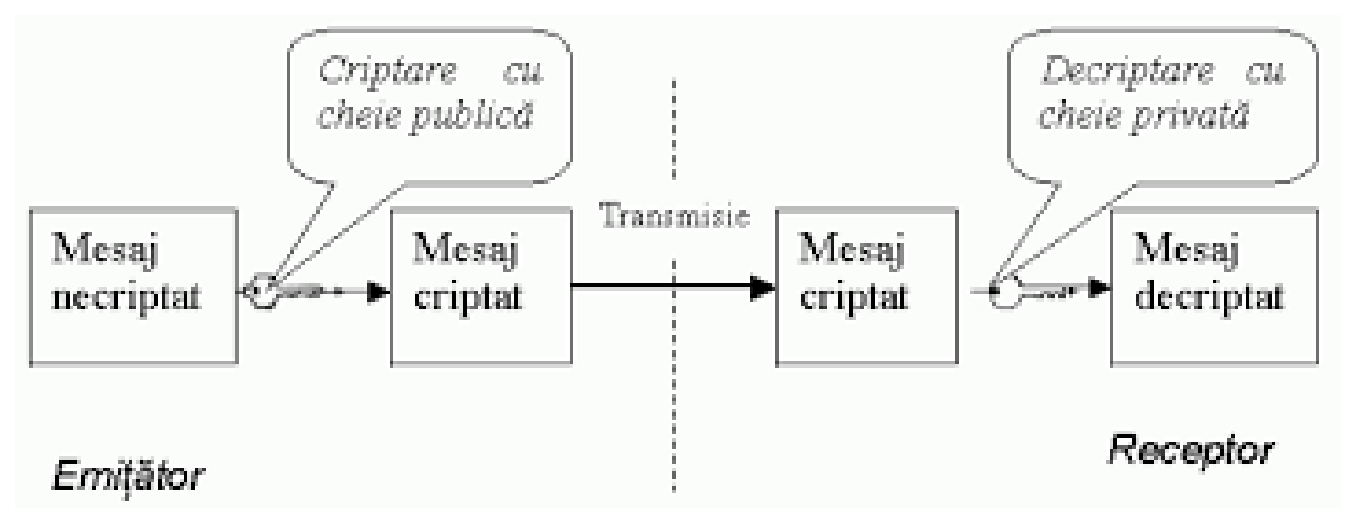
- Pentru protejarea informaţiilor sensibile se utilizează diferite forme de securitate, bazate pe criptare (în engleză, encryption), care reprezintă procesul de codificare a informaţiei astfel încât doar persoanele/computerele autorizate să poată descifra informaţia respectivă, cu ajutorul unei chei de decriptare.
- Conceptul de criptare există din cele mai vechi timpuri. De exemplu, generalii spartani foloseau criptarea pentru a transmite mesaje pe timp de război. În acest scop înfăşurau o hârtie în jurul unul cilindru de lemn şi scriau mesajul de-a lungul cilindrului, astfel, dacă mesajul era interceptat, inamicii erau nevoiţi să aibă un cilindru identic ca mărime pentru a putea citi informaţia.



- În general există două tipuri de criptare:
  - **Criptarea simetrică** - foloseşte o singură cheie de criptare/decriptare. Aplicația de criptare generează o cheie de criptare privată - poate fi o parolă sau un fişier de date - cu care se codifică informaţia dintr-un document. Accesarea documentului necesită rularea aceleiaşi aplicaţii de criptare şi cunoaşterea cheii de decriptare. Se recomandă transmiterea acestei chei printr-un canal securizat pentru a evita accesul persoanelor neautorizate. Criptarea simetrică prezintă avantajul că datele se criptează rapid, fiind utilizată în mod obișnuit în tranzacțiile electronice Dezavantajul constă în faptul că dacă se interceptează cheia de criptare, se pot accesa informațiile confidențiale. De asemenea, dacă se pierde cheia de criptare, datele devin inutilizabile



- **Criptarea asimetrică** sau bazată pe chei publice - este mult mai complexa şi mai sigură comparativ cu criptarea simetrică. Se foloseşte o pereche de chei de criptare - o cheie publică, cunoscută tuturor destinatarilor cu care se schimbă informaţii şi o cheie privată, cunoscută doar expeditorului. Acest sistem funcţionează ca un lacăt unde o cheie poate doar să închidă lacătul şi cealaltă cheie poate doar să deschidă lacătul.
- Altfel, cineva care doreşte să vă transmită informaţii criptate codifică datele cu cheia dumneavoastră publică. Doar cheia privată ce vă aparţine poate decodifica datele, cheia publică neputând face acest lucru, chiar dacă iniţial datele au fost criptate cu această cheie.



- Criptarea asimetrică necesită putere de procesare mult mai mare din cauza numerelor foarte mari folosite la cheile de criptare şi se foloseşte în certificate digitale, semnături digitale şi tranzacţii electronice.
- În cadrul procesului de criptare şi pentru protejarea informaţiilor sensibile se folosesc parole. Acestea se prezintă sub forma unui şir de caractere alfa-numerice şi simboluri care permit accesul la informaţii protejate şi diferite echipamente şi resurse de calcul. Cel mai des le întâlnim în cazurile de autentificare pe un calculator sau site web, unde avem nevoie de un nume de utilizator şi o parolă. Acestea sunt verificate cu datele dintr-un fişier securizat, iar dacă numele de utilizator sau parola nu se potrivesc, nu se permite accesul mai departe.

- La începuturile Internetului parolele erau stocate în clar într-o bază de date, însă, din cauza atacurilor electronice, parolele sunt criptate şi apoi stocate în baza de date, astfel, indiferent de ce se întâmplă, numai dumneavoastră veţi şti parola.
- Parolele stabilite trebuie concepute astfel încât să fie foarte greu de descoperit de către persoanele neautorizate. Pentru aceasta, se recomandă ca aceste parole să nu conțină date personale ale utilizatorului sau să nu fie parole generate automat de către calculator.
- Trebuie avut în vedere şi faptul că parolele sunt „case-sensitive", în sensul , că se face deosebire între caracterele majuscule şi cele minuscule folosite la scrierea parolei.
- De asemenea, este recomandat ca parolele să fie constituite dintr-o combinație de litere, cifre şi simboluri, să aibă o lungime corespunzătoare, să fie modificată la un anumit interval de timp şi, cel mai important, să nu fie comunicate altor persoane.

1.2.4. Înţelegerea caracteristicilor de bază legate de securitatea informaţiilor: confidenţialitate, integritate, disponibilitate

- Prin securitatea informaţiilor se înţelege protejarea informaţiei şi sistemelor Informatice ce asigură depozitarea informaţiilor, accesul şi transportul lor. Scopul esenţial în securitatea informaţiilor constă în asigurarea a 3 elemente esenţiale: confidenţialitate, integritate şi disponibilitate.
  - **Confidenţialitatea** se referă la asigurarea accesibilităţii informaţiilor doar pentru persoanele autorizate şi limitarea accesului persoanelor neautorizate. Asigurarea confidenţialităţii este critică în aplicaţiile care folosesc tranzacţii bancare online. O instituţie financiară ar trebui să ofere informaţii despre un anumit cont doar proprietarului contului respectiv. Confidenţialitatea este asigurată prin ***criptarea informaţiei***.
  - **Integritatea** se referă la măsurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate. Scopul menţinerii integrităţii datelor într-un sistem informatic este acela de a preveni afectarea datelor prin efectuarea de modificări necorespunzătare atât de utilizatorii autorizaţi, cât şi neautorizaţi. Integritatea datelor se obţine cu ajutorul unor ***algoritmi de verificare***.
  - **Disponibilitatea** se referă implicit la proprietatea unui sistem de a fi disponibil şi de a asigura accesul la informaţie utilizatorilor înregistraţi, atunci când aceasta este solicitată. Sistemele informatice care oferă informaţii pe Internet trebuie să asigure: disponibilitatea permanentă (sau pe o durată de timp cât mai mare), să prevină lipsa acesteia din diverse cauze (căderi de tensiune în reţeaua electrică, disfunţionalităţi hardware etc) prin diverse soluţii tehnice. Disponibilitatea este asigurată prin ***întărirea securităţii reţelei şi asigurarea existenţei unor copii de siguranţă***.

- Toate proprietăţile unui sistem - confidenţialitate, integritate şi disponibilitate sunt înrudite. Astfel, fără integritate, confidenţialitatea şi disponibilitatea unui sistem nu mai există deoarece, în momentul în care este posibilă efectuarea de operaţii necorepsunzătoare în cadrului unui sistem informatic, se pot crea uşor breşe de securitate în cadrul celorlalte proprietăţi. De asemenea, atacurile asupra disponibilității, activează anumite procese care pot slăbi integritatea sistemului.

1.2.5. Identificarea principalelor cerinţe legate de protecţia datelor/identităţii în ţara dvs.

- La nivel european, textul de referinţă în materie de protecţia datelor cu caracter personal este Directiva Europeană de Protecţie a Datelor din 1995. Aceasta instituie un cadru de reglementare menit să stabilească un echilibru între un nivel ridicat de protecţie a vieţii private a persoanelor şi libera circulaţie a datelor cu caracter personal în cadrul Uniunii Europene. Directiva esîe menită să protejeze drepturile şi libertăţile persoanelor în ceea ce priveşte ptelucrarea datelor cu caracter personal, stabilind limite stricte cu privire la colectarea și utilizarea datelor cu caracter personal. în plus, ea solicită ca fiecare stat membru să i creze un organism naţional independent responsabil cu protecţia unor astfel de date.
- Protecţia datelor cu caracter personal reprezintă un domeniu nou pentru spaţiul legislativ din România. Conţinutul său priveşte, într-o formă generică, dreptul persoanei fizice de a-i fi apărate acele caracteristici care conduc la identificarea sa şi obligaţia corelativă a statului de a adopta măsuri adecvate pentru a asigura o protecţie eficientă. în România, instituţia care asigură aplicarea dispoziţiilor normative anterior menţionate este Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, aceasta având competenţa de a investiga prelucrările de date cu caracter personal şi de a aplica sancţiuni, în cazul în care constată încălcarea dlipoilţlllor legale de către operatorii de date cu caracter personal, în urma sesizărilor din oficiu sau pe baza unor plângeri depuse de persoanele lezate în drepturile lor.

- Drepturile persoanelor ale căror date personale sunt colectate şi/sau prelucrate sunt:
  - Dreptul de acces la date
  - Dreptul de intervenţie asupra datelor
  - Dreptul de opoziţie
  - Dreptul de a nu fi supus unei decizii individuale
  - Dreptul de a se adresa justiţiei
- Obligațiile operatorilor de date cu caracter personal sunt:
  - Colectarea datelor în scopuri determinate, explicite şi legitime
  - Colectarea datelor adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate
  - Stocarea datelor într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate
  - Prelucrarea cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare a datelor cu caracter personal.

1.2.6. Înţelegerea importanţei creării şi aderării la liniile directoare şi politicile de utilizare TIC

- Aderarea la UE în 2007 a impus standarde mai stricte şi reglementări mai severe în toate domeniile, incluzând domenii-cheie precum tehnologia informaţiei. Elementele de bază ale legislaţiei TIC au fost adoptate în procesul de aderare la UE, sub forma adaptărilor naţionale ale directivelor elaborate de UE. În ceea ce priveşte mediul legislativ românesc în domeniul TIC, procesul de aliniere la reglementările Uniunii Europene a fost rapid şi eficient datorită unui sector de afaceri puternic şi a unei finanţări consistente vizând transferul de cunoştinţe (în domenii cum ar fi, spre exemplu, e-guvernarea, drepturile utilizatorilor de internet, securitatea datelor şi probleme privind gestionarea telecentrelor).
- Directivele UE în domeniul TIC oferă utilizatorilor un set de reguli standard ce definesc drepturile şi obligaţiile angajaţilor cu privire la utilizarea tehnologiei Informaţiei la locul de muncă, precum şi modul de utilizare al computerelor în vederea protejării datelor organizaţiei.