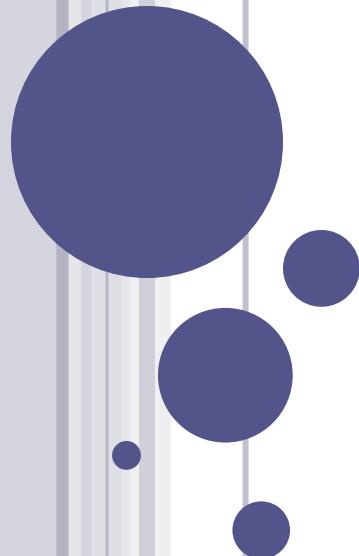


Cursul universitar
Gestiunea securității informative



Lidia Popov, dr., lect. univ.

Integrarea în programul de studii și structura cursului

Cursul este orientat spre înțelegerea, organizarea și asigurarea securității informațiilor, pornind de la cerințele pentru Sistemul de Management al Securității Informațiilor (SMSI), specificate în Organizația Internațională de Standardizare ISO/IEC 27001, analiza contextului organizației, stabilirea SMSI, identificarea și analiza riscurilor, alegerea măsurilor de asigurare a protecției informațiilor și terminând cu monitorizarea SMSI conform ciclului PDCA (Plan-Do-Check-Act).

Cursul universitar ***Gestiunea securității informative*** este un curs obligatoriu care include **150** de ore (**5 credite**): **40 de ore** contact direct (dintre ele **16 ore Prelegeri** și **24 de ore Laborator**) și **110 de ore** contact indirect.

Media aritmetică·0,5+Nota la examen·0,5 = Nota în matricolă



Plan

1. Introducere în securitatea informației

1.1. Servicii de securitate

1.2. Tipurile de infracțiuni și scopurile lor

1.3. Modalități de hacking sisteme informatice

1.4. Diverse atacuri

1.5. Obiectul de studiu al securității informațiilor

1.6. Atribute de securitate a informațiilor

1.7. Amenințări la adresa securității informației

1.8. Concluzii



Introducere în securitatea informației



Introducere

Una din caracteristicile societății moderne o reprezintă *informatizarea*. NTI sunt permanent implementate în diverse domenii ale activității umane. Prin utilizarea calculatoarelor și a soft-ului respectiv, sunt dirijate procese complexe din cele mai diverse domenii de activitate. Calculatoarele stau la baza multimilor de sisteme de prelucrare a informației, gestionează datele: păstrarea, prelucrarea informației și distribuirea ei către utilizator, realizând astfel TI moderne.

În fiecare an la **30 noiembrie** începând cu anul 1998, se sărbătorește **Ziua internațională pentru protecția informației**, care are scopul de a reaminti tuturor despre necesitatea de a proteja datele sensibile, precum și de a atrage atenția producătorilor și utilizatorilor asupra problemelor de securitate hardware și software.

Acest curs descrie aspectul juridic și organizatoric al asigurării securității informației, analiza vulnerabilităților și amenințărilor la adresa securității informației, metodele și mijloacele tehnice de protecție respective, fiind accentuate și problemele de securitate în rețelele de calculatoare.



Primele rețele de calculatoare au fost destinate pentru:

- ✓ schimb de documente prin intermediul poștei electronice, între cercetători, în instituțiile de învățământ superioare;
- ✓ imprimarea diferitor documente prin rețea la companii etc.

În schimb, sarcinile nu aveau vre-un impact referitor la securitatea datelor.



Actualmente

Milioane de oameni folosesc rețeaua de calculatoare pentru:

- ✓ gestionarea conturilor bancare;
- ✓ completarea declarației inspectoratului fiscal;
- ✓ procurarea de produse prin magazinele online;
- ✓ achitarea serviciilor comunale etc.

Problema securității informației devine
actuală!



Serviciul de securitate garantează:

- ✓ persoanele interesate de datele Dvs nu au acces pentru a citi sau a modifica mesajele care sunt destinate altor persoane;
- ✓ accesul la date îl au doar acele persoane care au careva drepturi;
- ✓ că mesajele trimise de unele persoane altor persoane sunt sigur trimise anume de acele persoane altor persoane.



Tipurile de infracțiuni și scopurile ei

Infractorul	Scopul
Student	Citirea din curiozitate a mesajelor altor persoane.
Hacker	Verificarea la siguranță a sistemului de securitate strain; de a fura datele.
Agent comercial	Se preface a fi agentul întregii Europe și nu doar a Moldovei.
Businessman	Vizionarea planurilor de marketing a concurenților
Angajat concediat	Răzbunarea pentru eliberarea din funcție a companiei
Contabil	Furtul banilor companiei
Broker	Nerespectarea promisiunii făcute clientului prin e-mail
Escroc	Furtul numărului cardului de credit pentru vînzare
Spion	Aflarea secretului comercial sau militar al inamicului
Terorist	Furtul secretului al armei bacteriologice

Modalități de hacking în sisteme informatiche

- ✓ Atacul la nivelul sistemului de operare;
- ✓ Atacul la soft-ul de rețea;
- ✓ Atacul la nivelul sistemelor de gestiune al BD etc.



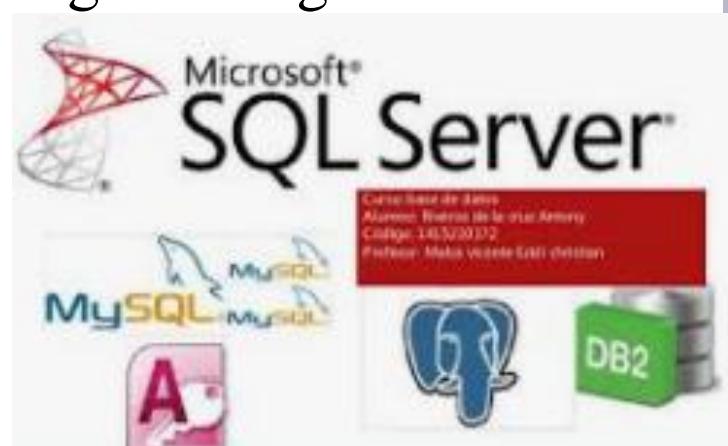
Atacul la nivelul SGBD

- ✓ Una din cele mai simple sarcini în securitatea datelor;
- ✓ SGBD are o structură internă bine definită și funcționare a elementelor bazelor de date care sunt definite destul de clar;
- ✓ Există patru operații de bază - căutarea, inserarea, ștergerea și înlocuirea elementelor;
- ✓ În cele mai multe cazuri, hackerii preferă să distrugă protecția unui sistem informatic la nivelul sistemului de operare (SO) și fișierele de acces de la bazele de date (BD) anume prin intermediul SO.



Atacul la nivelul SGBD

- ✓ Există două scenarii de atac asupra BD:
 - rezultatele de operații aritmetice asupra numerelor în SGBD este rotunjit cu lipsă, iar diferența rezultantă este înscrisă într-o altă înregistrare a BD;
 - hackerul obține acces la câmpurile înregistrărilor SGBD doar cu informațiile statistice disponibile.
- ✓ Ideea unui atac hacker asupra unei BD – se reduce la formularea unei astfel de interogări, astfel ca rezultatul să prezinte doar informație statistică, constând dintr-o singură înregistrare.



Atacul la nivelul sistemului de operare

- ✓ Structura internă a SO moderne este extrem de complexă și, prin urmare, respectarea politicii de securitate adecvată este mai dificilă;
- ✓ Atacul constă doar în găsirea unui punct slab într-un sistem concret de securitate;
- ✓ Implementarea cu succes a unui algoritm de atac în practică depinde în mare măsură de arhitectura și configurarea SO concret, care este obiectul atacului.



Furtul parolei

- ✓ Spionarea utilizatorului care culege parola, care oferă dreptul de a lucra cu SO;
- ✓ Obținerea parolei dintr-un fișier, în care parola a fost salvată;
- ✓ Găsirea parolei pe care utilizatorul, pentru a nu o uita, o înscrie în calendar sau în agende sau pe partea din spate a tastaturii calculator.



Furtul parolei

- ✓ Furtul dispozitivului extern de memorie cu informație despre parole;
- ✓ Generarea tuturor paralelor posibile;
- ✓ Potrivirea parolei după frecvența de apariție a caracterelor și bigramelor folosind dicționare cu cele mai frecvent folosite parole, care implică cunoștințe despre utilizatorul sistemului.



Scanarea discurilor rigide (HardDisk)

- ✓ Apel secvențial la fiecare fișier din memorie;
- ✓ Verificarea spațiului disponibil pe dispozitivul de memorie;

Colectarea „gunoiului” (spațiului de memorie rezervat)

- ✓ Verificarea obiectelor șterse din coșul de gunoi de alți utilizatori ai sistemului.



Extinderea drepturilor de acces

- ✓ Hackerii depășesc drepturile care le sunt conferite în cadrul politicii de securitate actuale al sistemului:
 - rularea programului, din numele utilizatorului care are autoritatea necesară sau asemănător unui program de sistem;
 - înlocuirea bibliotecii dinamice încărcate de soft-ul de sistem sau modificarea variabilelor de sistem care descriu calea de la această bibliotecă;
 - modificarea codului sau a datelor subsistemului de securitate al SO etc.



Refuz de la întreținerea sistemului

- ✓ Preluarea resurselor sistemului;
- ✓ Atac cu interogări;
- ✓ Folosirea erorilor în aplicația respectivă sau în administrarea sistemului etc.;



- ✓ Dacă sistemul nu conține erori și administratorul respectă strict politica de securitate recomandată de producătorii SO, atunci atacurile vor fi ineficiente;
- ✓ Măsurile de securitate trebuie să fie luate în dependență de fiecare sistem în parte.



Atac la software-ul de rețea

- ✓ Canal de comunicare prin care sînt transmise mesajele de cele mai multe ori nu sunt protejate;
- ✓ Oricine poate avea acces la canal, respectiv, poate intercepta și trimite aceste mesaje;



Atac la software-ul de rețea

- ✓ Preluarea unui segment LAN;
- ✓ Interceptarea mesajelor pe router;
- ✓ Crearea unui router fals;
- ✓ Impunerea mesajelor;
- ✓ Refuz la întreținere etc.

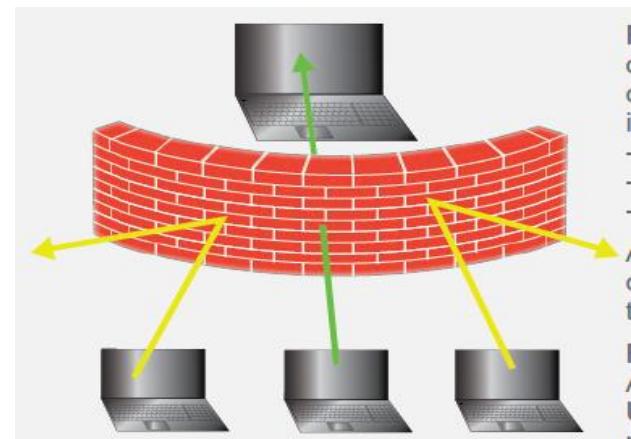


Exemple de securizare a rețelei

- ✓ Reducerea maximală a dimensiunii rețelei;
- ✓ Criptarea mesajelor din rețea (adică să codifice în aşa mod informația, astfel încât să poată fi înțeleasă doar de persoanele autorizate);
- ✓ Utilizarea semnăturii digitale pentru mesajele din rețea;
- ✓ Utilizarea firewall-ului.

Firewall-ul sau ***paravanul de protecție*** este un dispozitiv sau o serie de dispozitive cu rolul de a cripta, filtra sau intermedia traficul între diferite domenii de securitate pentru a ține la distanță traficul de Internet cu intenții rele:

- viermii și anumite tipuri de virusi;
- hackerii etc.



Firewall-ul protejează calculatorul împotriva accesărilor neautorizate. Aceste accesări pot fi realizate prin intermediul porturilor de date.

Un **firewall** cooperează cu un program de routare, care verifică fiecare pachet de date din rețea ce va trece prin serverul gateway (poartă), pentru a hotărî dacă va fi trimis mai departe sau nu.

Prin folosirea unui **firewall** aveți posibilitatea de a seta excepții sau de a bloca traficul de date al anumitor aplicații în funcție de caz.



Exemple:

Presupunem că s-a descărcat un joc care pentru a rula necesită conectarea la Internet. Acest lucru înseamnă că jocul folosește trafic de date. Când veți încerca să deschideți jocul, se va deschide în primul rând paravanul de protecție care Vă va întreba ce acțiune doriți să aveți asupra jocului.

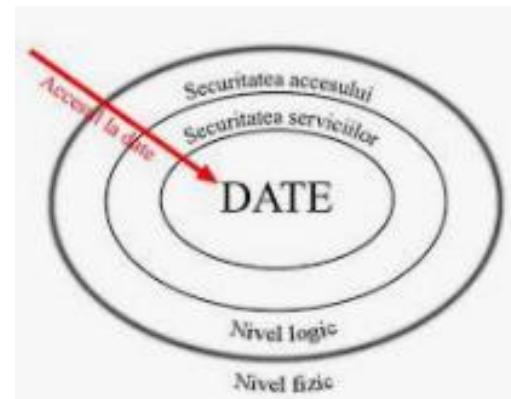
Aveți de ales două opțiuni:

1. Puteți să alegeti opțiunea de a adăuga jocul la *excepții*, ceea ce înseamnă că i se acordă jocului posibilitatea de a se conecta la Internet și acesta se va deschide rulând normal;
2. Puteți să *blocați jocul*, ceea ce înseamnă că jocul nu se va conecta la Internet și în concluzie nu se va deschide.



Recomandări pentru asigurarea securității sistemului (12)

1. Fiți la curent cu cele mai recente evoluții din domeniul securității informației.
2. Acceptați principiul suficienței rezonabile: nu depune eforturi pentru o protecție totală de securitate.
3. Păstrați în secret informațiile confidențiale cu privire la principiile mecanismelor de securitate ale sistemului informatic.



Recomandări pentru asigurarea securității sistemului

4. Reduceți la maximum dimensiunea rețelei securizate.
5. Amplasați serverele în încăperile protejate fără a fi unite la tastatură și mouse.
6. Criptați absolut toate mesajele transmise prin canale de comunicare nesecurizate și obligator să conțină semnătura digitală.



Recomandări pentru asigurarea securității sistemului

7. Nu neglijați serviciul de audit.
8. Verificați periodic integritatea programelor de soft.
9. Toate politicile de securitate le înregistrați în registrele hârtie (varianta scriptică).
10. Securitatea să fie la un nivel înalt cu SO sigure.
11. Creați mai multe capcane pentru atacatori.
12. Testați regulat utilizând programe speciale.



Obiectul de studiu al securității informațiilor

Securitatea informației este un proces care are scopul de a asigura protecția informației de acțiuni neautorizate la adresa acesteia. **De exemplu:** accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea neautorizată a informației.

Tehnicile de asigurare a securității pot fi aplicate la orice informație, indiferent de natura ei, și este important de remarcat că informația are valoare, în special, atunci când ea este subiectul schimbului sau procesării, și anume, în cazul în care este vulnerabilă (poate fi atacată ușor/părți slabe) în fața unor părți ce nu pot fi considerate *de încredere*.



Astfel, fără a exclude valoarea informației stocate, valoarea acesteia crește evident în acțiunea de schimb sau în acțiunea de procesare și este evident că o informație complet izolată, nu conduce la riscuri de securitate foarte mari, dar, în același timp, nici nu poate aduce foarte multe beneficii, având, în general, valoare scăzută.



Securitatea informației* vizavi de *Securitatea informatică

Securitatea informației

Ramură a informaticii ce se ocupă cu identificarea riscurilor implicate de folosirea dispozitivelor informative: calculatoarele, smartphone-urile, rețelele de calculatoare atât publice, cât și private și cu oferirea de soluții pentru înlăturarea acestor riscuri.

Securitatea informatică

Caracterizează un domeniu mai îngust, calculatoarele fiind doar o componentă a sistemelor informatice.

Securitatea informației

Include protecția informației pe orice suport, nu neapărat digital și este dependentă nu numai de tehnica de calcul, ci și de infrastructura conexă, cum ar fi, de exemplu, sistemele de alimentare cu energie, apă, căldură, aparate de aer condiționat, mijloace de comunicare, resursele umane etc.

În același timp, o noțiune mai generală este ***Securitatea informațională***, care denotă protejarea atât a informației, cât și a sistemelor informatice care, la rândul său, asigură depozitarea, accesul și transportul informațiilor.



Ce este securitatea informațională?



Securitatea informațională

Securitatea informațională se ocupă de protejarea informației și a sistemelor informatice, de accesul neautorizat, de folosirea, dezvăluirea, întreruperea, modificarea și distrugerea acestora etc.

Securitatea informațională, la fel ca și protecția datelor, este o sarcină complexă, care are scopul furnizării securității, realizabilă prin implementarea unui sistem de securitate.



Securitatea informațională

Protecția datelor este o problemă multilaterală și complexă, care cuprinde o serie de sarcini importante. Problema securității informaționale se agravează permanent din cauza pătrunderii mijloacelor tehnice de prelucrare și transfer de date și mai ales a sistemelor de calcul, în toate domeniile societății.

Astăzi, există *trei principii de bază*, pe care trebuie să le furnizeze securitatea informatională:

- ✓ integritatea datelor - protecția împotriva erorilor, care duc la pierderea de informații și protecția împotriva creării sau distrugerii neautorizate a datelor;
 - ✓ confidențialitatea informației;
 - ✓ accesul către informație pentru toți utilizatorii autorizați.



Informația

este un produs care, ca și alte produse importante rezultate din activitatea umană, are valoare și, în consecință, este necesar să fie protejată corespunzător, iar aceasta se realizează prin:

Măsuri organizatorice

Includ măsuri îndreptate împotriva distrugerii cauzate de catastrofele naturale, măsuri referitoare la selecția profesională a personalului, organizarea unui sistem de control al accesului, organizarea păstrării și utilizării suporturilor de informații etc.

Măsuri juridice

Cuprind documente normative ce verifică și reglementează procesul prelucrării și folosirii informației.

Măsuri și mijloace informatice sau tehnice

Constituite din echipamente, programe și tehnici de protecție.

Atribute de securitate a informațiilor

Atributele de securitate sunt niște însușiri esențiale ale informației, care o fac mai puțin vulnerabilă la atacurile de securitate, a căror țintă este această informație. Acestea mai sunt numite și proprietăți, obiective de securitate, concepte fundamentale de securitate, criterii sau caracteristici critice ale informației.



*Securitatea informației este
tratată prin cele trei
componente principale,
numite atrbute primare de
securitate ale informațiilor.*



Atributele primare de securitate a informațiilor

Confidențialitatea

Asigurarea accesului la informații numai pe baza drepturilor de acces aprobate ale persoanei, în acord cu nivelul de secretizare a informației accesate și a permisiunii rezultate din aplicarea principiului nevoii de a cunoaște.

Integritatea

Interdicția modificării, prin ștergere sau adăugare sau a distrugerii, în mod neautorizat, a informațiilor. Adică datele să nu poată fi falsificate decât de persoane autorizate.

Disponibilitatea

Asigurarea condițiilor necesare regăsirii și folosirii cu ușurință a informațiilor ori de câte ori este nevoie, cu respectarea strictă a condițiilor de confidențialitate și integritate.

Triada CIA



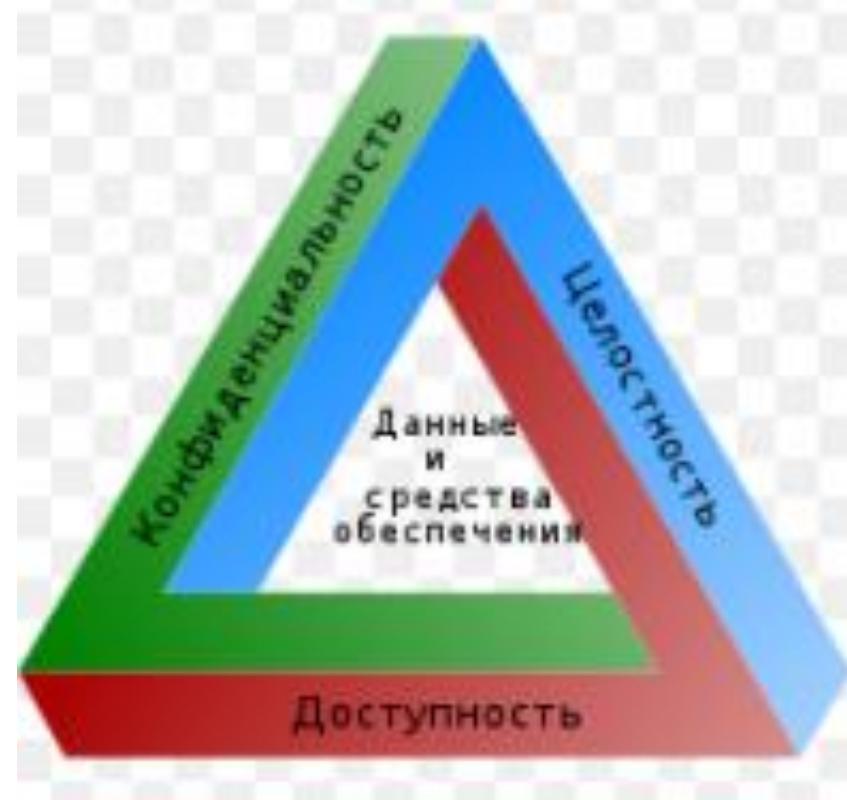
C – presupune interzicerea accesului neautorizat al persoanelor la informația care nu le este destinată și de care ele nu au nevoie pentru îndeplinirea unor sarcini de serviciu.

I – înseamnă că datele să nu poată fi alterate sau să nu poată fi modificate decât de persoane autorizate.

D – prezintă asigurarea utilizatorilor legali cu informația completă, în cazul în care aceștia au nevoie de ea, iar utilizatorii trebuie să aibă acces doar la datele care le sunt destinate.



În contextul triadei CID, *Securitatea informației* poate fi definită ca ansamblul măsurilor și structurilor îndreptate spre protecția informațiilor sociale, prelucrate sau transmise prin intermediul sistemelor informative și de comunicații sau al altor sisteme, precum și împotriva amenințărilor și a oricărora acțiuni, care pot afecta CID informației sau funcționarea sistemelor informative, indiferent dacă acestea apar accidental sau intenționat.



Exemple

C: este o componentă necesară a vieții private și se referă la capacitatea noastră de a ne proteja datele de cei care nu sunt autorizați să le vizualizeze. Cazul unei persoane care retrage bani de la un ATM (bancomat), persoana în cauză va încerca să păstreze **C** numărului personal de identificare (PIN), care îi permite, în combinație cu cardul bancar, să extragă banii de la bancomat etc.

I – este deosebit de importantă, în cazul în care se referă la datele care reprezintă fundamentul pentru unele decizii, cum ar fi cazul unui atacator care ar modifica datele care conțin rezultatele testelor medicale, s-ar putea ca medicul să prescrie greșit tratamentul, care ar putea duce la moartea pacientului.

D – asigurarea condițiilor necesare de a regăsi și de a folosi cu ușurință diverse informații.

Confidențialitate vizavi Securitate

Diferența dintre *confidențialitate* și *securitate* poate fi puțin confuză, deoarece securitatea și confidențialitatea sunt doi termeni interdependent.

În lumea TI, asigurarea securității înseamnă furnizarea a trei servicii de securitate: *confidențialitate*, *integritate* și *disponibilitate*. Confidențialitatea înseamnă păstrarea unui secret în cazul în care secretul este cunoscut doar de părțile vizate. Tehnica cea mai utilizată pentru asigurarea confidențialității este *criptarea*.



Ce este Securitatea?

Securitatea se referă la asigurarea confidențialității, integrității și disponibilității a trei servicii. *Confidențialitatea* este una dintre aceste servicii de securitate.

Altfel spus, *securitatea* este un termen umbrelă în care confidențialitatea face parte din ea.

Asigurarea securității poate fi mai costisitoare decât asigurarea confidențialității, deoarece securitatea implică și alte servicii decât confidențialitatea.

O încălcare a vieții private înseamnă o încălcare a securității, pe când o încălcare a securității nu înseamnă întotdeauna o încălcare a vieții private.



Ce este Confidențialitatea?

Confidențialitatea este unul dintre cele mai importante lucruri în furnizarea securității. **Dacă există o încălcare a confidențialității, securitatea este afectată.**

Așadar, confidențialitatea face parte din securitate. Securitatea presupune furnizarea de servicii cum ar fi confidențialitatea, integritatea și disponibilitatea, iar confidențialitatea este un astfel de serviciu care intră sub incidența securității. De ex., în cazul în care într-o companie, sediu central comunică prin intermediul Internet-ului cu sucursala. Dacă unii hackeri pot obține informații sensibile, atunci confidențialitatea este pierdută. Tehnicile, precum criptarea, sunt folosite pentru a proteja intimitatea.



Ce este Confidentialitatea?

Angajații de pe ambele părți cunosc o cheie secretă pe care numai ei o știu și orice comunicare poate fi decodificată numai folosind acea cheie. Acum un hacker nu poate obține acces la informații fără cheie. Aici, intimitarea depinde de păstrarea secretului cheii. **Confidentialitatea** poate fi cu privire la o singură persoană. O persoană poate avea date de care are nevoie pentru a-și păstra privat pentru sine. Deci, și în această situație, criptarea poate ajuta la asigurarea confidențialității.



Autenticitatea, responsabilitatea și non-repudierea (ARN-R)

Odată cu atingerea nivelului înalt de informatizare pe care îl are societatea modernă, la conceptele fundamentale care alcătuiesc Triada CID, au mai fost alăturate ARN-R, fără de care asigurarea nivelului corespunzător de protecție a informației devine dificilă.



Asigurarea nivelului corespunzător de protecție a informației

Autenticitatea

Asigurarea că datele, tranzacțiile, comunicațiile sau documentele (în format electronic sau fizic) sunt autentice. De asemenea, este important să fie validat faptul că ambele părți implicate sunt cine pretind a fi.

Responsabilitatea

Un concept esențial de securitate a informațiilor și denotă că fiecare persoană, care lucrează cu un sistem informatic, trebuie să aibă responsabilități specifice pentru asigurarea informațiilor. Persoana responsabilă de securitatea informațiilor trebuie să efectueze verificări periodice pentru a se asigura că politica este urmată.

Non-repudierea

O măsură, prin care se asigură faptul că, după emiterea sau recepționarea unei informații într-un sistem de comunicații securizat, expeditorul sau destinatarul nu poate nega, în mod fals, că a expediat sau a primit informațiile în cauză.

Non-repudierea

Non-repudierea își propune să confirme destinatarului unui mesaj electronic faptul că acest mesaj este scris și trimis de persoana care pretinde că l-a trimis. În acest fel, se asigură încrederea părților.

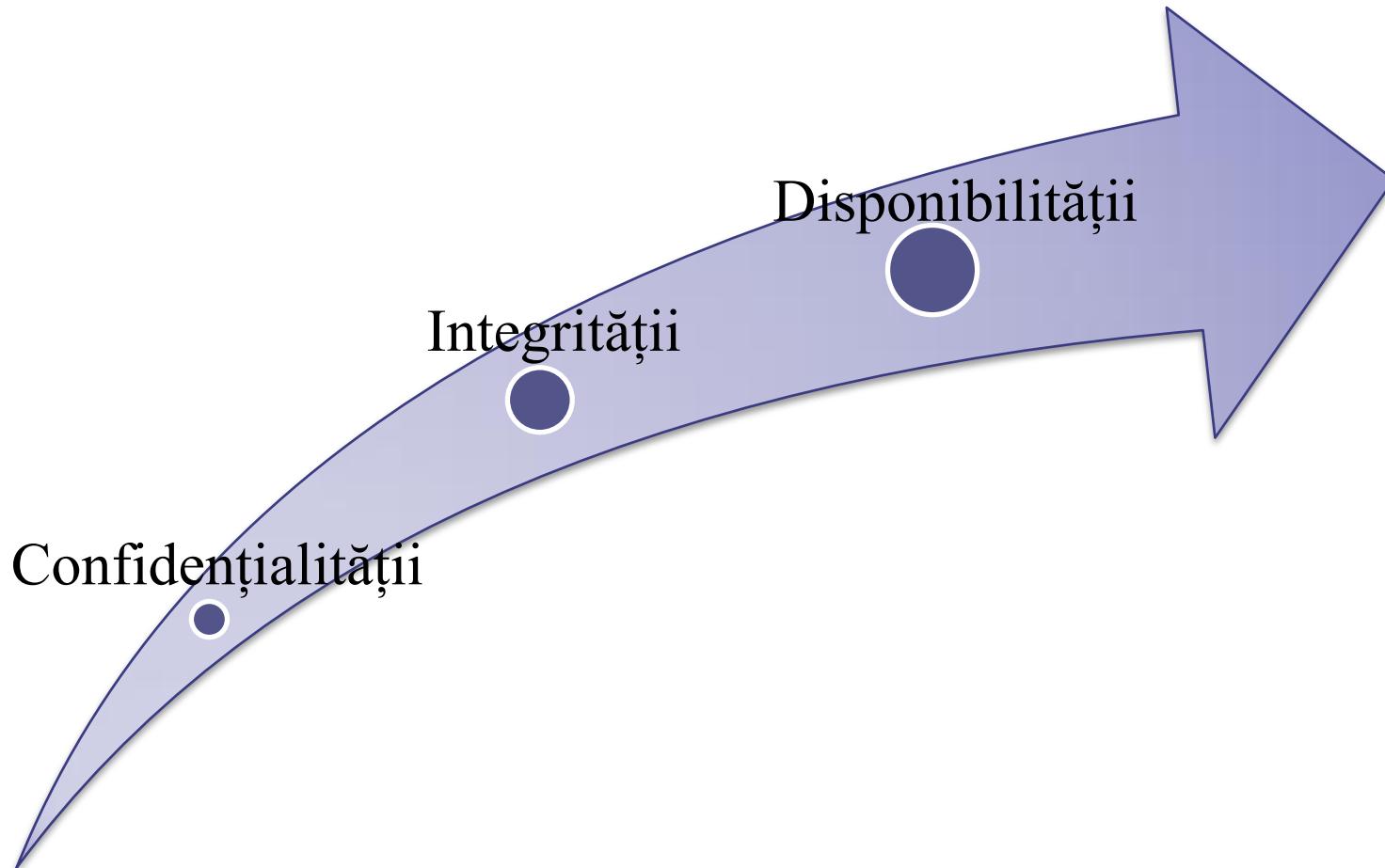
Non-repudierea stă la baza semnăturilor digitale, asigurând autenticitatea acestora, adică este un aspect important al semnături digitală - prezintă o schemă matematică folosită pentru a demonstra autenticitatea mesajelor sau documentelor digitale.

O semnătură digitală validă oferă destinatarului o bază solidă pentru a crede că mesajul a fost creat de către un expeditor cunoscut (autentificare), să fie sigur că expeditorul nu poate nega că a trimis mesajul (non-repudiere), și că mesajul nu a fost modificat pe parcurs (integritate).



Amenințări la adresa securității informației

Accentul este plasat pe amenințări la adresa:



Ce înțelegem prin
amenințare la
adresa securității
informației?



Amenințarea la adresa securității informației este intenția, acțiunea sau inacțiunea manifestate real sau potențial, sau factorul cu caracter ecologic, tehnic sau de alt gen, a cărui realizare sau dezvoltare contravine sau poate să contravină intereselor legale de bază ale persoanei, societății și statului în spațiul informațional.

În conformitate cu standardul ISO/IEC 27005, *amenințarea* este cauza potențială a unui incident nedorit, care poate provoca daune unui sistem sau unei organizații. O tentativă de a pune în aplicare amenințarea se numește *atac*, cel care face o astfel de încercare - *atacator*. Atacatorii potențiali sunt numiți *surse de amenințare*.

Amenințarea este un rezultat al *vulnerabilității*, adică al slăbiciunii unei resurse sau grup de resurse, care poate fi exploarată de una sau de mai multe amenințări.



Amenințările la adresa securității informației pot fi clasificate în conformitate cu următoarele criterii:

Aspectul securității informației (CID) spre care amenințările, în primul rând, se îndreaptă

Componentele sistemelor informaticice, care sunt obiectul amenințărilor (date, software, echipament, infrastructură)

Metoda de realizare (acțiuni accidentale/intenționate naturale/provocate de om)

Amplasarea sursei amenințării (în interior/afara sistemului)

Amenințări la adresa **Confidențialității**

Informația confidențială poate fi împărțită în două categorii:

Informație de serviciu
(parolele)

Informație de domeniu

Informația de serviciu nu se referă la un anumit domeniu, în sistemul informatic aceasta joacă un rol tehnic, însă divulgarea ei este deosebit de periculoasă, deoarece, în consecință, se poate obține accesul neautorizat la toate informațiile, inclusiv și la cele din domeniu.

Furtul de echipamente, de asemenea, este o amenințare a confidențialității, atât pentru unitățile de stocare externe, cât și pentru calculatoare, în general, în special pentru cele portabile.

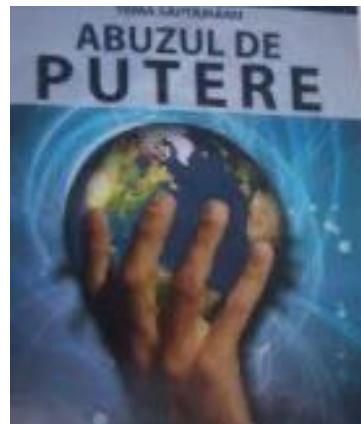
O amenințare periculoasă a confidențialității, ce nu ține de metodele tehnice, este *mascarada* – realizarea de activități sub masca unei persoane cu autoritatea de **acces la date**.



Abuzul de putere

Abuzul de putere este o amenințare de care este dificil de protejat. În multe tipuri de sisteme, utilizatorul privilegiat (administratorul de sistem), are posibilitatea de a citi orice fișier (necriptat), poate avea acces la e-mailul oricărui utilizator etc.

Un alt exemplu constă în cauzarea daunelor în timpul deservirilor tehnice. În mod normal, inginerul de la service primește acces nelimitat la echipament și este capabil de a ocoli mecanismele de protecție ale software-ului.



Amenințări la adresa Integrității

Integritatea poate fi:

Statică

Încălcarea integrității statice – introducerea datelor incorecte sau modificarea datelor. Pot fi falsificate, de exemplu, antetele de e-mail, întreg mesajul poate fi falsificat de către o persoană care cunoaște parola.

Dinamică

Aplicarea corectă a acțiunilor complexe (tranzacții). Amenințări ale integrității dinamice sunt: furtul, reordonarea, duplicarea datelor sau introducerea de mesaje suplimentare etc. Mijloacele de control ale integrității dinamice se aplică, în special, la analiza fluxului de mesaje financiare.

Amenințări la adresa Disponibilității

Se clasifică după componentele sistemului informatic la care se referă amenințarea:

Refuzul utilizatorului

Refuzul de a lucra cu sistemul informatic; incapacitatea de a lucra cu sistemul din cauza lipsei de pregătire corespunzătoare și a lipsei de suport tehnic etc.

Defectul intern al sistemului informatic

Devierea de la normele de funcționare stabilite; ieșirea sistemului din modul normal de funcționare; erorile în configurarea sistemului; defecțiuni hardware și software; distrugerea datelor; distrugerea sau deteriorarea echipamentului.

Refuzul infrastructurii sistemului

Perturbări ale sistemului de comunicații, de alimentare cu energie electrică sau termică, apă, aer condiționat; distrugerea sau deteriorarea încăperilor etc.

Concluzii

- ✓ Securitatea informației ține mai mult de persoanele concrete decât repararea erorilor de sistem;
- ✓ Problemele securității informației, la rândul său, țin de:
 - **Confidențialitate** - înseamnă prevenirea situației în care informația de contact ajunge în mâinile utilizatorilor neautorizați;
 - **Autentificare** vă permite să stabiliți cu cine vorbiți înainte de a da altor persoane accesul la informații sau să se alăture cu el înr-o relaie de afaceri.

Concluzii

Confidențialitatea și autentificarea asigură punerea în aplicare strictă a angajamentelor și a integrității sistemului.



Multumim pentru atenție!

