Slide 2: **Obiective:**

- Definirea noțiunii de securitate cibernetică și a elementelor acesteia
- Identificarea modalităților utilizate pentru a securiza informatiile, aplicațiile si rețelele WI-FI
- Stabilirea importanței securității cibernetice

Slide 3: Astăzi, Internetul este utilizat pentru a face publicitate și a vinde produse sub diverse forme, pentru a comunica cu clienții și comercianții cu amănuntul și pentru a efectua tranzacții financiare. Din această cauză, hackerii și infractorii cibernetici folosesc internetul ca instrument de răspândire a programelor malware și de atacuri cibernetice.

Securitatea cibernetică își propune să protejeze computerele, rețelele și programele software de astfel de atacuri cibernetice. Majoritatea acestor atacuri digitale vizează accesarea, modificarea sau ștergerea de informații sensibile, extragerea de bani de la victime sau întreruperea operațiunilor normale de afaceri. Securitatea cibernetică se clasifică în următoarele tipuri:

Slide 4: Siguranța informațiilor vizează protejarea informațiilor personale ale utilizatorilor împotriva accesului neautorizat, a furtului de identitate. Protejează confidențialitatea datelor și a hardware-ului care manipulează, stochează și transmit aceste date. Exemple de securitate a informațiilor includ autentificarea utilizatorilor și criptografia.

Slide 5: Securitatea informațiilor este caracterizată prin trei componente principale: confidențialitatea, integritatea și disponibilitatea. Confidențialitatea este asigurată prin criptarea informației. Integritatea se obține prin mecanisme și algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță.

Slide 6: Securitatea aplicațiilor vizează protejarea aplicațiilor software de vulnerabilitățile care apar datorită defectelor din fazele de proiectare, dezvoltare, instalare, upgrade sau întreținere a aplicațiilor.

Slide 7: Confidentialitatea

Confidentialitatea comunicarii implica ca datele schimbate între un client si un furnizor sa nu poata fi citite de catre un tert. Criptarea este tehnologia de baza pentru schimbul de mesaje confidentiale de pe canalele nesigure de comunicatie. Dintre abordarile cele mai comune, mentionam utilizarea canalelor private sau retelelor private virtuale (VPN).

- **Integritatea**

Notiunea stricta de integritate se refera la faptul ca nimeni nu trebuie sa modifice schimbul de informatii. În ceea ce priveste comunicarea pe retelele nesigure, accesibile publicului, falsificarea nu poate fi exclusa, în general, dar este posibila detectarea datelor modificate.

- **Non-repudierea**

Non-repudierea este un aspect important al contractelor electronice. Autorii mesajelor (de exemplu, clientii care comanda carti la un magazin online) nu ar trebui sa aiba posibilitatea sa refuze comenzile realizate de acestia.

- **Autentificarea**

Autentificarea este procesul de verificare a identitatii unei persoane sau a unui subiect general (care poate fi o alta aplicatie care invoca un serviciu în numele unui utilizator uman). Autentificarea are loc de cele mai multe ori printr-un mecanism de login/parola. Deoarece tehnologiile (cum sunt serviciile web) sunt proiectate pentru comunicarea aplicatie-la-aplicatie inter-organizationala si nu se bazeaza pe interactiunea cu utilizatorul uman, autentificarea bazata pe chei publice devine, în aceasta situatie, foarte importanta.

- **Autorizarea**

Autorizarea este utilizata pentru a decide ce privilegii vor fi acordate utilizatorilor autentificati. Autorizarea poate depinde de identitatea solicitantilor si/sau de atributele lor caracteristice, cum este vârsta (de exemplu, în cazul unui magazin on-line specializat pe distribuirea de filme). Listele de control al accesului (ACL) sunt folosite pe scara larga, desi reprezinta o tehnica destul de precara pentru o organizatie.

- **Disponibilitatea**

Garantarea disponibilitatii aplicatiilor web are o relevanta economica, deoarece nefunctionarea serviciilor implica pierderi financiare.

- **Intimitatea**

Intimitatea se refera la manipularea datelor de încredere, cum ar fi informatiile cu caracter personal (de exemplu, datele de contact sau numerele cardurilor de credit), dar si la fisierele stocate în sistemul de fisiere local. Aceste date nu trebuie sa fie accesibile pentru parti terte neautorizate, care ar putea abuza de acestea prin furtul de identitate.

Slide 8: Criptarea este o tehnologie de baza care permite schimbul securizat de mesaje. Criptare (sau cifrarea) implica utilizarea de functii matematice prin care un simplu text este transformat într-un text cifrat. Decriptarea (sau decifrarea) descrie procesul invers, adica transformarea textului codificat înapoi în textul original simplu. Cei mai multi algoritmi de criptare se bazeaza pe chei secrete pentru cifrare si decifrare. Fara a cunoaste cheile respective, sistemele de calcul nu pot decripta mesajele, desi cei mai puternici algoritmi de criptare sunt accesibili publicului. Analiza criptarii descrie eforturile si tehnologiile implicate pentru a "sparge" o criptare (de exemplu, prin gasirea modalitatilor de a sparge o criptare pe baza unui text cifrat si a textului

simplu corespunzator). Un algoritm este considerat puternic, în cazul în care o cautare "brute force" (adica, procesul de încercare a oricarei chei posibile), este singura posibilitate de atac cunoscuta. În continuare vom discuta algoritmii de criptare simetrici si asimetrici.

Slide 9: Siguranța rețelei vizează protejarea utilizării, integrității și siguranței unei rețele, a componentelor asociate și a datelor distribuite în rețea. Atunci când o rețea este asigurată, amenințările potențiale sunt blocate de la intrarea sau răspândirea în acea rețea. Exemple de securitate în rețea includ programe Antivirus și Antispyware, Firewall care blochează accesul neautorizat la o rețea și VPN-uri (Virtual Private Networks) folosite pentru acces securizat la distanță.

Slide 10: Caracteristici de securitate:

- autentificarea,
- confidențialitatea
- integritatea,
- disponibilitatea
- controlul accesului
- administrarea cheilor
- managementul securității

Slide 11: Prima tehnică de criptare a cadrelor la nivelul legătură de date a fost WEP (*Wired Equivalent Privacy*), numele sugerând că a fost gândită cu scopul de a obține o securitate a legăturii de date echivalentă cu cea a unei rețele Ethernet. Această tehnică fost folosită din 1997 până când a fost spartă în 2001 și a încetat să mai fie considerată sigură din 2005 odată cu publicarea standardului de securitate IEEE 802.11i.

WPA și WPA2 pot funcționa în două moduri distincte. Cel mai simplu dintre acestea, folosit în general la rețele personale (casnice sau ale unor firme mici), presupune configurarea stațiilor cu ajutorul unei parole de acces, parolă din care se calculează cheile de criptare cu ajutorul funcției PBKDF (*Password-Based Key Derivation Function*). În celălalt mod, WPA2 autentifică stațiile de lucru cu ajutorul unui server RADIUS.

Slide 12: Concluzie:

Atacurile cibernetice continuă să evolueze. Nu numai că observăm o creștere a atacurilor cibernetice asupra întreprinderilor și persoanelor fizice, dar și nivelul de sofisticare a acestora a

crescut . În anii care vor veni, vor exista atacuri cibernetice și mai avansate, folosind noi tehnologii, victime și intenții. Observăm necesitatea unor măsuri mai bune de securitate cibernetică în rândul organizațiilor de toate tipurile. Astfel, ar trebui să existe un plan adecvat și metode puternice pentru securitatea cibernetică pentru a preveni și atenua daunele atacurilor cibernetice.