**(slide 6) Criptografia**

Criptografia este o ramura a matematicii care se ocupa cu securizarea si autentificarea accesului intr-un sistem informatic. Prin intermediul unui algoritm sau al unei serii de operatii matematice, un text simplu este transformat intr-un text cifrat, iar aceasta poate fi realizata prin metode matematice sau prin metode de criptare cuantica. Criptarea este procesul de transformare a textului clar in text cifrat, iar decriptarea este opusul sau. Sistemele criptografice necesita o anumita metoda pentru ca destinatarul sa poata utiliza mesajul criptat, de obicei prin transformarea textului cifrat in text clar. Criptografia este utilizata in securitatea informatiilor, inclusiv in protectia datelor personale si a informatiilor financiare. Cheia este o alta informatie, aproape intotdeauna un numar, care specifica modul in care algoritmul este aplicat textului clar pentru a-l cripta. Intr-un sistem criptografic sigur, chiar metoda prin care este criptat un mesaj este cunoscuta, dar ar trebui sa fie dificil sau imposibil de decriptat fara cheia respectiva.

**(slide 10) Tipuri de documente electronice**

Cateva dintre tipurile de documente utilizate frecvent includ documente text care conțin doar text și sunt create cu ajutorul unui software de procesare a textului precum Microsoft Word și sunt salvate în formate de fișier precum DOCX sau RTF. Foile de calcul sunt utilizate pentru organizarea și analizarea datelor în format tabelar, cum ar fi situațiile financiare și listele de inventar și sunt create cu ajutorul unui software precum Microsoft Excel și sunt salvate în formate de fișier precum XLSX sau CSV. Prezentările sunt utilizate pentru a crea prezentări vizuale care includ text, imagini și elemente multimedia, cum ar fi cele audio și video, și sunt create cu ajutorul unui software precum Microsoft PowerPoint și sunt salvate în formate de fișier precum PPTX sau PDF.

PDF-urile sunt utilizate pentru partajarea documentelor online si pot include text, imagini si elemente multimedia.

Cartile electronice sunt versiuni digitale ale cartilor care pot fi citite pe dispozitivele electronice si sunt create cu ajutorul unor programe specializate.

Imaginile sunt fisiere digitale care contin continut vizual static sau animat, cum ar fi fotografii, ilustratii si logo-uri.

Fisierele audio si video contin continut audio sau video, cum ar fi muzica, podcast-uri si filme.

Documentele de proiectare sunt utilizate in procesul de proiectare si dezvoltare a produselor si serviciilor.

Markdown si LaTeX sunt limbaje utilizate pentru crearea documentelor text simple sau complexe, utilizate in special in contexte academice si stiintifice.

**(slide 13, 14) Riscurile si amenintarile**

Accesul neautorizat:

Accesul neautorizat se refera la obtinerea accesului la un sistem sau serviciu fara permisiunea adecvata.

Poate aparea prin ghicitul parolelor sau incercarea de a accesa zone restrictionate ale sistemului.

Sistemele securizate pot bloca accesul sau pot alerta administratorii in cazul incercarilor de acces neautorizat.

Virusi si malware:

Virusii informatici sunt programe malware care se ataseaza la alte documente sau programe si se pot raspandi in sistem.

Pot distruge date, incetini sistemul sau colecta informatii personale.

Atacurile cu virusuri si malware pot duce la pierderea de date, furtul de informatii personale si infectarea intregului sistem.

Atacurile cibernetice si man-in-the-middle:

Atacurile cibernetice vizeaza obtinerea controlului sau accesului la documente si sisteme importante.

Pot include atacuri DDoS, phishing, injectarea SQL, scripturi intre site-uri si atacuri botnet.

Scopul poate fi distrugea datelor sau obtinerea de informatii clasificate.

Atacul "man-in-the-middle" permite unui atacator sa intercepteze si sa modifice comunicarea dintre un utilizator si un sistem.

Acest atac este dificil de realizat in prezent, datorita utilizarii masive a protocolului HTTPS.

Expunere accidentala sau intentionata:

Expunerea accidentala sau intentionata a informatiilor din documentele electronice poate duce la pierderea datelor si incalcarea confidentialitatii.

Poate aparea prin trimiterea gresita a unui e-mail sau incarcarea incorecta a unui document.

Angajatii rau intentionati sau partenerii de afaceri pot divulga informatii sensibile.

Scaderea performantei sistemului informatic:

Scaderea performantei sistemului poate duce la pierderea sau coruperea datelor si la incapacitatea de a executa sarcinile importante.

Poate fi cauzata de erori de programare, suprasolicitare a sistemului, virusi informatici sau probleme hardware.

Este important sa se ia masuri pentru a preveni si a proteja impotriva acestui risc.

**(slide 15) Masuri de protectie si securitate pentru documentele electronice**

Autentificare si autorizare:

Autentificarea si autorizarea sunt esentiale pentru securitatea documentelor electronice. Utilizarea factorilor precum parole, autentificarea in doi factori si biometria ajuta la protejarea documentelor.

Criptarea:

Criptarea datelor implica transformarea lor intr-un cod necitibil fara cheia corecta, pentru a proteja informatiile sensibile in timpul transmiterii electronice. Criptarea nu garanteaza securitatea absoluta si trebuie completata cu alte masuri. Implementarea corecta si protectia cheilor sunt esentiale.

Criptarea AES:

AES (Advanced Encryption Standard) este un algoritm comun de criptare, utilizat pe scara larga, ce utilizeaza o matrice de stare 4x4 si o serie de pasi, cum ar fi adaugarea cheii de runde, substitutia octetilor si combinatia coloanelor, pentru a cripta un bloc de 16 octeti. AES-256 este cea mai sigura varianta, dar necesita mai multa putere de calcul. Criptarea AES utilizeaza aceeasi cheie pentru criptare si decriptare. Este importanta utilizarea criptarii AES pentru a proteja datele in repaus si in miscare, cum ar fi informatiile personale, datele medicale si inregistrarile financiare.

* As mai mentiona despre metoda de criptare XchaCha20 care in multe moduri, este asemanatoare cu cea prezentata anterior, AES, fiind pe 256 biti, simetric, cu o cheie pentru codificare si decodificare. Diferenta interesanta consta in modul de criptare a bitului, in loc de diviziare a datelor in blocuri, acesta cripteaza in mod distinct fiecare bit. Pe scurt, rezulta o viteza mai rapida de procesare si este mai putin complex. De asemenea, nu are nevoie de hardware specializat si nu este asa de predispus la erori umane.

**(slide 18) Semnatura electronica si digitala**

Semnatura electronica si digitala reprezinta metode utilizate pentru a autentifica documentele electronice. Semnatura digitala este mai sigura, deoarece este legata criptografic de document si poate fi verificata. Este sustinuta de un certificat digital emis de o terta parte de incredere si ofera dovezi puternice privind identitatea semnatarului si integritatea documentului. In schimb, semnatura electronica poate fi o imagine sau un simbol care nu este insotita de o dovada de identitate.

Semnaturile digitale se bazeaza pe cheile publice si private si necesita protejarea acestora pentru a evita falsificarea sau utilizarea malefica. Autoritatile de Certificare (CA) sunt organizatii recunoscute care asigura securitatea cheilor si furnizeaza certificate digitale.

Politiciile si procedurile de securitate in cadrul unei companii sunt esentiale pentru protejarea documentelor electronice si a altor informatii sensibile. Acestea trebuie sa acopere aspecte precum accesul la date, protejarea parolelor, utilizarea dispozitivelor mobile, utilizarea e-mailului, transferul de date, protectia impotriva amenintarilor cibernetice si monitorizarea si auditarea. Actualizarea regulata a acestor politici si proceduri este importanta pentru a se adapta la noile amenintari cibernetice si tehnologice.