7. Securitatea cibernetică și protejarea datelor

Într-o lume digitalizată, securitatea cibernetică și protejarea datelor au devenit priorități esențiale pentru afaceri. Platformele online gestionează volume mari de informații sensibile, inclusiv date personale și financiare ale clienților. Asigurarea unui mediu sigur pentru aceste date este crucială pentru câștigarea încrederii clienților și pentru protejarea afacerii împotriva amenințărilor cibernetice.

7.1 Importanța Securității Cibernetice în contextual digital

Securitatea cibernetică reprezintă ansamblul de practici, tehnologii și măsuri utilizate pentru protejarea sistemelor informatice, a rețelelor și a datelor împotriva atacurilor și accesului neautorizat.

Pentru antreprenorii care își digitalizează afacerea, protejarea informațiilor sensibile este esențială pentru a evita pierderi financiare și de reputație.

Informația sensibilă reprezintă orice tip de date care, dacă sunt accesate, modificate sau divulgate fără permisiune, pot cauza prejudicii unei persoane sau unei organizații. Aceasta poate include:

- ✓ Date personale – nume, adresă, cod numeric personal, date de contact.
- ✓ Informații financiare – detalii despre conturi bancare, tranzacții, date ale cardurilor de credit.
- ✓ Proprietate intelectuală – brevete, modele de afaceri, inovații și date de cercetare.
- ✓ Date despre clienți și angajați – istoricul comenzilor, preferințele clienților, contractele de muncă.
- ✓ Informații comerciale confidențiale – strategii de afaceri, rapoarte financiare, analize de piață.

Protejarea acestor date este esențială pentru menținerea încrederii și securității în cadrul unei afaceri.

Majoritatea persoanelor au o percepție eronată asupra riscurilor de securitate cibernetică, considerând că acestea afectează doar marile companii sau instituțiile guvernamentale.

Consecințele atacurilor cibernetice

- ✓ Atacurile cibernetice pot avea consecințe grave asupra persoanelor și organizațiilor.
- ✓ Breșa de securitate poate duce la pierderea clienților și la deteriorarea imaginii companiei.
- ✓ Atacurile cibernetice pot cauza pierderi financiare uriașe, fie prin furtul de date, fie prin oprirea operațiunilor.
- ✓ Costurile asociate recuperării datelor, plății ransomware-ului sau reparării sistemelor pot fi semnificative.

În realitate, atacatorii vizează orice utilizator sau afacere, indiferent de dimensiune, exploatând vulnerabilități precum parole slabe, lipsa actualizărilor software sau necunoașterea metodelor de atac.

7.2 Principalele amenințări la adresa securității informaționale

1. **Atacuri de tip malware**

- Viruși, troieni și ransomware care infectează dispozitivele și criptează datele utilizatorilor pentru a solicita o răscumpărare.

Malware- orice program sau cod creat cu intenția de a deteriora, fura date sau compromite sistemele informatice.

Există numeroase tipuri de malware, însă cele mai cunoscute sunt virușii și troienii, pe care probabil le-ați întâlnit deja. Vă recomandăm să puneți pauză și să faceți cunoștință cu diferite tipuri de malware.

În continuare vă vom prezenta scenarii care vă vor ajuta să recunoașteți situații de risc.Se atașează la fișiere legitime și se răspândește odată cu deschiderea acestora. Poate șterge date sau afecta funcționalitatea sistemului.

- ✓ **Virus**
  Se atașează la fișiere legitime și se răspândește odată cu deschiderea acestora. Poate șterge date sau afecta funcționalitatea sistemului.
- ✓ **Troian**
  Se deghizează în software legitim, dar oferă atacatorilor acces neautorizat la sistem.
- ✓ Ransomware
  Blochează accesul la fișiere și solicită o răscumpărare pentru decriptare.
- ✓ **Spyware**
  Monitorizează activitatea utilizatorului și fură date sensibile, inclusiv parole și informații bancare.
- ✓ **Worms**
  Se răspândesc automat în rețea fără a necesita acțiunea utilizatorului, exploatând vulnerabilitățile sistemului.
- ✓ **Adware**
  Afișează reclame agresive și poate colecta date despre comportamentul utilizatorului.

Orice tip de fișier poate conține un virus, fie că este o imagine, un videoclip, un fișier PDF sau o aplicație. Unele dintre acestea devin periculoase imediat ce ajung pe dispozitiv, putând fi activate fără a necesita deschiderea de către utilizator. Astfel, trebuie să fim foarte atenți în privința la cum accesăm, deschidem sau descărcăm un fișier.

2. Phishing

- Metode de inginerie socială utilizate pentru a înșela utilizatorii să furnizeze informații sensibile, cum ar fi parole sau detalii financiare.
  - ✓ Smishing (SMS Phishing)
    Atacatorii folosesc mesaje SMS pentru a trimite linkuri malițioase sau pentru a convinge utilizatorii să furnizeze informații confidențiale.
  - ✓ Vishing (Voice Phishing)
    Phishing prin apeluri telefonice, în care atacatorii se dau drept reprezentanți ai unei instituții de încredere și cer utilizatorului să divulge informații sensibile.
  - ✓ Angler Phishing
    Atac realizat prin intermediul rețelelor sociale, în care atacatorii creează conturi false și răspund la comentarii sau mesaje private, pretinzând că oferă suport tehnic sau asistență oficială.
  - ✓ Search Engine Phishing
    Atacatorii creează site-uri false care apar în rezultatele motoarelor de căutare pentru anumite căutări populare.

În 2022, EasyDMARC a raportat că Moldova s-a clasat în top 5 țări cele mai vizate de atacurile de phishing prin e-mail, alături de Țările de Jos, Rusia, SUA și Thailanda. Potrivit datelor analizate, Moldova a primit peste 27 milioane de e-mailuri malițioase, reprezentând aproximativ 6,98% din totalul atacurilor de phishing identificate la nivel global.

Protejarea afacerii de phishing: Măsuri tehnice de securitate

- ✓ Folosirea sistemelor de operare și a software-ului licențiat.
- ✓ Utilizarea soluției antivirus integrate în sistemul de operare.
- ✓ Limitarea accesului la date sensibile, permițând doar persoanelor autorizate să efectueze operațiuni critice.

Protejarea afacerii de phishing: Instruirea și conștientizarea angajaților

- ✓ Toți membrii echipei trebuie să înțeleagă cum arată un e-mail suspect și să nu acceseze linkuri necunoscute.
- ✓ Organizați traininguri periodice pentru a-i ajuta să recunoască tentativele de phishing.
- ✓ Focusați-vă asupra directorilor executivi și persoanele cuprinsă între 31-50 de ani.

3. Atacuri aasupra site-ului Web

- Site-urile web sunt frecvent ținta atacurilor cibernetice care urmăresc fie compromiterea securității, fie accesul neautorizat la datele utilizatorilor. În continuare vă prezentăm câteva tipuri de atacuri frecvente.
  - ✓ Atacuri DDoS reprezintă generarea unui volum mare de cereri către server pentru a-l supraîncărca și a-l face inaccesibil utilizatorilor legitimi.
  - ✓ Atacurile prin injecție reprezintă metode utilizate de atacatorii cibernetici pentru a introduce cod malițios într-o aplicație web sau într-o bază de date, exploatând vulnerabilitățile existente.
  - ✓ Atacul de tip defacement implică accesul ilegal la un site și înlocuirea conținutului original cu mesaje malițioase, propagandă, conținut ofensator sau imagini specifice atacatorilor.
  - ✓ Atacul de tip pharming implică redirecționarea utilizatorilor către site-uri malițioase prin compromiterea serverelor DNS sau modificarea fișierelor locale de sistem.

Atacurile asupra site-urilor web pot compromite datele utilizatorilor, afecta funcționalitatea platformei și provoca pierderi financiare. Protejarea unui site împotriva acestor amenințări necesită implementarea unor măsuri de securitate cibernetică eficiente și administrarea lor de către specialiști cu expertiză în domeniu.

Un specialist IT poate asigura protecția site-ului prin implementarea unor soluții avansate de securitate, adaptate specificului platformei. Alegerea unui furnizor de hosting cu măsuri de securitate robuste contribuie semnificativ la reducerea riscurilor asociate atacurilor cibernetice.

4. Accesul neautorizat

- Hackeri sau angajați rău-intenționați care accesează datele sau sistemele fără permisiune.

5. Breșe de securitate în lanțul de aprovizionare

- Atacurile indirecte care vizează furnizorii sau partenerii unei companii pentru a obține acces la datele sale.

7.3 Păstrarea și protejarea datelor

Monitorizarea continuă este esențială pentru prevenirea incidentelor. Scanările periodice pentru identificarea vulnerabilităților, verificarea log-urilor și efectuarea testelor de penetrare permit detectarea și remedierea rapidă a amenințărilor, asigurând astfel funcționarea optimă a site-ului.

Protejarea datelor este esențială pentru securitatea unei afaceri și respectarea reglementărilor privind confidențialitatea.

Baza de date este componenta centrală a oricărei afaceri care gestionează informații digitale. Copiile de siguranță ale datelor sunt necesare pentru recuperarea rapidă în cazul unui atac cibernetic, defecțiuni hardware sau erori umane.

Un backup automat și periodic trebuie realizat la intervale regulate, astfel încât datele să fie mereu actualizate și să poată fi recuperate în cazul unui incident.

Pentru a preveni accesul neautorizat sau compromiterea datelor, backup-urile trebuie stocate în medii sigure și protejate prin criptare, fie pe servere separate, fie în soluții de stocare în cloud.

Pe lângă realizarea copiilor de siguranță, este esențială și testarea periodică a backup-urilor pentru a verifica integritatea acestora și a asigura că restaurarea poate fi efectuată fără probleme în situații critice. O strategie eficientă de backup reduce riscurile asociate pierderii de date și contribuie la continuitatea operațiunilor.

Datele trebuie gestionate conform principiilor de securitate și confidențialitate pentru a preveni utilizarea neautorizată.

Protejarea datelor necesită implementarea unor măsuri de securitate eficiente pentru a preveni accesul neautorizat și compromiterea informațiilor sensibile.

7.4 Măsuri de securitate informațională

1) Măsuri tehnice

- Sisteme de criptare: Protejarea datelor sensibile atât în tranzit, cât și în repaus.
- Firewall-uri: Monitorizarea și filtrarea traficului de rețea pentru a preveni accesul neautorizat.
- Antivirus și anti-malware: Detectarea și eliminarea programelor malițioase.
- Backup-uri regulate: Salvarea periodică a datelor pentru a preveni pierderea informațiilor în caz de atacuri.

Pe lângă protecția tehnică, respectarea reglementărilor privind confidențialitatea datelor și conformitatea legală, cum ar fi Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană, care asigură că datele sunt manipulate într-un mod care protejează drepturile individuale și limitează accesul neautorizat. Organizațiile care nu respectă aceste reglementări riscă sancțiuni financiare mari și pierderea reputației.

2) Educația utilizatorilor

- Organizarea de traininguri pentru angajați cu privire la bunele practici de securitate cibernetică, precum recunoașterea atacurilor de tip phishing.
- Conștientizarea importanței utilizării parolelor complexe și a autentificării în doi pași.

- Dezvoltarea unei culturi organizaționale care prioritizează securitatea, prin formarea continuă a angajaților despre practici de securitate și prin menținerea unor protocoale stricte de securitate.

3) **Politici și procese interne**

- Implementarea de politici clare privind accesul la date și utilizarea dispozitivelor de serviciu.
- Audituri periodice de securitate pentru a identifica și remedia vulnerabilitățile.

4) **Utilizarea tehnologiilor avansate**

- Sisteme de detectare a intruziunilor (IDS): Monitorizarea traficului de rețea pentru a identifica activități suspecte.

5) **I și machine learning:** Identificarea și prevenirea automată a amenințărilor bazate pe comportamente anormale

Exemplu de bună practică

- Platforma e-comerț poate utiliza certificatul SSL pentru a asigura siguranța tranzacțiilor online și a proteja datele financiare ale clienților.

Studii de caz

1. Atacul asupra Marriott International (2018)

- Breșă care a expus informațiile personale ale peste 500 de milioane de utilizatori.
- Lecție: Importanța segmentării bazelor de date și a monitorizării continue a accesului.

2. Colonial Pipeline (2021)

- Atac ransomware care a dus la oprirea temporară a unei conducte critice din SUA.
- Lecție: Necesitatea implementării unor măsuri stricte de securitate pentru infrastructuri critice.

7.4 Beneficiile unei bune securități informaționale

- **Protecția reputației:** O companie cu o bună securitate informațională își poate păstra încrederea clienților.
- **Creșterea competitivității:** Oferirea unui mediu sigur pentru utilizatori și parteneri poate diferenția compania pe piață.
- **Reducerea costurilor:** Prevenirea atacurilor cibernetice reduce pierderile financiare și costurile de remediere.
- **Conformitatea cu reglementările:** Respectarea legislației în vigoare elimină riscul amenzilor și sancțiunilor.

Exemple

- **Amazon u**tilizează autentificarea cu mai mulți factori și tehnologie avansată de criptare pentru a proteja datele clienților și tranzacțiile financiare.
- **PayPal o**feră un sistem securizat de plată, protejând atât datele financiare ale utilizatorilor, cât și tranzacțiile efectuate.

Concluzii

Protejarea datelor necesită implementarea unor măsuri precum criptarea, anonimizarea și restricționarea accesului, pentru a preveni utilizarea neautorizată.

Monitorizarea și prevenția sunt esențiale pentru detectarea activităților suspecte și reducerea riscurilor de compromitere a informațiilor.

O infrastructură digitală sigură protejează atât datele utilizatorilor, cât și reputația organizației, contribuind la încrederea și continuitatea operațională.