Cofinanțat de Uniunea Europeană

Proiectul Wallachia e-Hub este finanțat prin Digital Europe Programme (EC/101083410) - WeH și prin Programul Creștere Inteligentă, Digitalizare și Instrumente Financiare (POCIDIF/1147/2/1/161799)

WALLACHIA eHUB ROADSHOW

WEH.SPIRUHARET.RO

**MARIUS MIHĂILESCU,**
TRAINER COORDONARE A TRANSFORMĂRII DIGITALE

# Securitatea datelor, vulnerabilități și atacuri informatice în contextul administrației publice

EDIH European Digital Innovation Hubs Network

Proiectul WE HUB for digital transformation

În era digitală actuală, securitatea datelor reprezintă un aspect critic pentru orice organizație, inclusiv pentru administrațiile publice. Protecția informațiilor sensibile și prevenirea atacurilor cibernetice sunt esențiale pentru menținerea încrederii publice și pentru asigurarea continuității serviciilor guvernamentale.

OBIECTIVE

- Conștientizarea vulnerabilităților: Identificarea și înțelegerea principalelor vulnerabilități cibernetice.
- Analiza atacurilor informatice: Examinarea tipurilor comune de atacuri și impactul lor asupra administrațiilor publice.
- Strategii de securitate: Prezentarea celor mai bune practici și soluții pentru protejarea datelor.

**1. Vulnerabilități Cibernetice în Administrația Publică**

- Sistemele IT învechite. Lipsa actualizărilor software și utilizarea unor tehnologii depășite;
- Acces neautorizat. Practici slabe de gestionare a parolelor și lipsa autentificării multi-factor;
- Erori umane. Lipsa instruirii adecvate a personalului și neatenție și manipulare greșită a datelor.

**2. Tipuri de Atacuri Informatice**

- Atacuri phishing. Metode de inginerie socială pentru obținerea de informații confidențiale;
- Malware și ransomware. Software rău intenționat care compromite sau criptează datele;
- Atacuri DDoS (Distributed Denial of Service). Supraincarcarea serverelor pentru a întrerupe serviciile;
- Exploatarea vulnerabilităților. Utilizarea breșelor de securitate pentru acces neautorizat.

**3. Impactul Atacurilor Informatice**

- Perturbarea serviciilor publice: Întârzieri și întreruperi în furnizarea serviciilor esențiale;
- Pierderi financiare: Costuri legate de restaurarea sistemelor și pierderea veniturilor;
- Compromiterea datelor: Scurgerea de informații sensibile și impact asupra confidențialității;
- Afectarea reputației: Pierderea încrederii publicului și a partenerilor.

**4. Strategii și măsuri de securitate**

- Implementarea sistemelor moderne de securitate. Actualizări regulate ale software-ului și utilizarea soluțiilor avansate de securitate;
- Formarea și educația angajaților. Programe continue de instruire în securitatea cibernetică;
- Politici și proceduri de securitate. Stabilirea și aplicarea politicilor stricte de acces și gestionare a datelor;
- Utilizarea tehnologiilor de monitorizare. Implementarea soluțiilor de monitorizare și detectare a intruziunilor.

Securitatea datelor în administrația publică este o provocare continuă care necesită atenție constantă și adaptare la noile amenințări. Prin înțelegerea vulnerabilităților, recunoașterea tipurilor de atacuri și adoptarea celor mai bune practici de securitate, administrațiile publice pot proteja informațiile sensibile și asigura funcționarea eficientă a serviciilor pentru cetățeni.