GUVERNUL REPUBLICII MOLDOVA

TEHNICI ȘI TEHNOLOGII DE GUVERNARE ELECTRONICĂ

CURS UTM
FCIM ANUL IV

LECȚIA 10:
SECURITATEA CIBERNETICĂ ÎN CONTEXTUL SERVICIILOR ELECTRONICE

1. SECURITATEA CIBERNETICĂ
2. PROTECȚIA DATELOR, INCLUSIV A CELOR CU CARACTER PERSONAL

LECTOR: IURIE ȚURCANU, Centrul de Guvernare Electronică

CHIȘINĂU
17 NOIEMBRIE, 2016

CONȚINUTUL CURSULUI

1. Noțiuni fundamentale de guvernare electronică
2. Ciclul de viață a serviciilor electronice
3. Tipuri de servicii electronice
4. Elemente arhitecturale ale serviciilor electronice
5. Documentul electronic. Semnătura electronică
6. Plăți electronice. Comerț electronic. Monedă electronică.
7. Cadrul de interoperabilitate/schimb de date.
8. Tehnologii Cloud computing
9. **Securitatea cibernetică**
10. Guvernare deschisă. Date deschise.

SECURITATEA CIBERNETICĂ

- Prin **securitatea cibernetică** se înțelege totalitatea de tehnologii și procese menite să protejeze computerele, rețelele, serviciile și datele de acces neautorizat, vulnerabilități și atacuri inițiate de persoane cu rea intenție prin Internet.
- **Securitatea comunicației** – protejarea mediilor de comunicații, tehnologiilor aferente comunicațiilor și a conținutului în cadrul organizației
- **Securitatea rețelelor** – protejarea componentelor de rețea, a conexiunilor și a conținutului
- **Securitatea informației** – protejarea informației și a elementelor critice ale acesteia, inclusiv a componentelor hardware și software care utilizează, stochează sau transmit această informație.

CRIME CIBERNETICE

- Crimă cibernetică – activitate ilegală cu caracter distructiv cu utilizarea mijloacelor și tehnologiilor TIC, care are ca scop distrugerea, alterarea sau compromiterea serviciilor și/sau datelor.
- Crimele cibernetice includ, dar nu se limitează la:
  - Acces ilegal la informații/servicii
  - Interceptare ilegală de date
  - Indisponibilizare parțială sau totală a sistemelor/serviciilor
  - Alterare sau indisponibilizare a datelor
  - Fraude

SECURITATEA DATELOR

- Furt/divulgare de date
  - Accesarea neautorizată a datelor cu regim restricționat de acces
  - Publicarea datelor clasate
  - Datele rămân integre și disponibile
- Alterarea datelor
  - Integritatea datelor este compromisă și datele nu mai pot servi ca informație de încredere
  - Fiind alterate, datele oricum rămân disponibile
- Indisponibilitatea datelor
  - Datele nu sunt accesibile pentru consum

MĂSURI DE SECURITATE CIBERNETICĂ ÎN CONTEXTUL SERVICIILOR ELECTRONICE

- Autentificarea și autorizarea utilizatorilor
- Integritatea datelor și a serviciilor
- Disponibilitatea datelor și serviciilor
- Confidentialitea informației
- Dreptul la viața privată
- Non-repudierea

AUTENTIFICAREA, AUTORIZAREA ȘI NON-REPUDIEREA

- **Autentificarea** – presupune verificarea identităţii utilizatorului, de obicei, pe baza de nume si parola. Ea raspunde la întrebarea fundamentală : „cine este acest utilizator?” , şi reprezintă procesul care identifică in mod unic clienţii deserviţi de aplicaţie sau servicii.

- **Autorizarea** - specifica acţiunile pe care un utilizator le poate realiza intr-un anumit context. Aceasta este asociată autentificarii. Ea raspunde la întrebarea: ce poti face ? şi reprezintă procesul care guvernează ce resurse sau operaţii poate accesa userul care este autentificat. Resursele includ fişiere , baze de date, tabele, recorduri, şamd impreună cu resurse sistem cum ar fi registry keys sau date de configurare.
- **Non-repudierea** - asigură că expeditorul unui mesaj nu poate afirma că nu l-a trimis

INTEGRITATEA ȘI DISPONIBILITATEA DATELOR ȘI A SERVICIILOR

- **Integritatea datelor și a serviciilor** - presupune detectarea incercărilor de modificare neautorizată a datelor transmise. Aceasta reprezintă garanţia că datele sunt protejate împotriva modificărilor accidentale sau (răuvoitoare)deliberate. La fel ca şi privacy, integritatea este o preocupare cheie, in special, când datele sunt transmise prin mai multe reţele. Integritatea datelor în tranzit este de obicei asigurată prin utilizarea tehnicilor de hashing şi a codurilor de autentificare a mesajelor.
- **Disponibilitatea** – o anumită resursă este necesar să fie accesată la momentul oportun.

CONFIDENȚIALITATEA INFORMAȚIEI ȘI DREPTUL LA VIAȚA PRIVATĂ

- **Confidentialitatea**
  - Imposibilitatea unei terţe entităţi sa aibă acces la datele vehiculate între doi receptori. Este procesul care asigură că datele ramân confidenţiale şi că nu pot fi accesate de către utilizatori neautorizaţi sau de cei care monitorizeaza fluxul de date intra si inter reţele.
  - Criptarea este utilizată in mod frecvent pentru a asigura confidentialitatea.

- **Dreptul la viața privată** – vizează drepturile ce trebuie respectate privind caracterul (subiectul) datelor vehiculate. Aceasta este deseori confundată cu confidenţialitatea.

VĂ MULȚUMIM!

Informație de contact:
E-mail: office@egov.md