Cofinanțat de Uniunea Europeană

Proiectul Wallachia eHUB (WEH)
ID proiect: EC/101083410 – WeH; POCIDIF/1147/2/1/161799

Str. Italiană nr. 28, sect. 2, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Sesiune de Instruire în Cybersecurity pentru Administrații Publice

Marius Iulian Mihăilescu, Dr. Ing.

Trainer coordonare a transformării digitale

m.mihailescu.mi@spiruharet.ro
+40755 834 679 (WhatsApp)

EDIH European Digital Innovation Hubs Network

Proiectul WE HUB for digital transformation

01 Importanța securității cibernetice în administrația publică

Necesitatea protejării datelor sensibile

Riscurile asociate cu atacurile cibernetice

Atacurile cibernetice pot compromite informații sensibile ale cetățenilor, afectând încrederea în administrația publică.

Conformitatea cu reglementările legale

Administrațiile publice trebuie să se conformeze legislației privind protecția datelor, asigurând astfel securitatea informațiilor personale.

Impactul asupra serviciilor publice

O breșă de securitate poate întrerupe serviciile publice esențiale, afectând astfel funcționarea normală a administrației.

Educarea angajaților în privința securității cibernetice

Importanța formării continue

Angajații trebuie să fie instruiți constant pentru a recunoaște amenințările cibernetice și a lua măsuri preventive eficiente.

Simularea atacurilor cibernetice

Prin simulări, angajații pot învăța cum să reacționeze în caz de atac, îmbunătățind astfel reacția la incidentele reale.

Promovarea unei culturi de securitate

Crearea unei culturi de securitate cibernetică în cadrul instituției este esențială pentru protejarea datelor și a sistemelor.

Tehnologii avansate pentru securitate cibernetică

1

Implementarea soluțiilor de criptare

Criptarea datelor ajută la protejarea informațiilor sensibile în cazul în care acestea sunt compromise de atacatori.

2

Utilizarea sistemelor de detecție a intruziunilor

Sistemele de detecție a intruziunilor monitorizează activitatea rețelei pentru a identifica și răspunde rapid la amenințări.

3

Actualizări constante ale software-ului

Menținerea software-ului actualizat este crucială pentru a preveni exploatarea vulnerabilităților cunoscute de către atacatori.

02 Identificarea amenințărilor cibernetice comune pentru primării

Principalele tipuri de atacuri cibernetice

Atacurile de tip phishing

Atacurile de tip phishing vizează obținerea de informații sensibile prin înșelăciune, folosind email-uri false sau site-uri compromițătoare.

Ransomware-ul

Ransomware-ul criptează datele instituției și cere o răscumpărare pentru deblocarea acestora, afectând grav funcționarea primăriei.

Atacurile DDoS

Atacurile DDoS inundă serverele primăriei cu trafic, provocând oprirea serviciilor online și afectând accesibilitatea pentru cetățeni.

Impactul amenințărilor cibernetice asupra primăriilor

Perturbarea serviciilor publice

Amenințările cibernetice pot duce la sistarea serviciilor publice esențiale, afectând accesibilitatea cetățenilor la informații și servicii.

Pierderea datelor sensibile

Furtul datelor personale sau financiare poate avea consecințe juridice și reputaționale grave pentru primărie și cetățeni.

Costuri financiare mari

Atacurile cibernetice generează costuri semnificative pentru recuperarea datelor, îmbunătățirea securității și gestionarea incidentelor.

Măsuri de prevenire a amenințărilor cibernetice

1

Formarea angajaților

Este esențial ca angajații să fie instruiți în identificarea amenințărilor cibernetice și să utilizeze practici de securitate eficiente.

2

Implementarea de soluții de securitate

Utilizarea unor soluții avansate de securitate cibernetică, cum ar fi firewall-uri și software antivirus, protejează infrastructura digitală.

3

Evaluarea periodică a riscurilor

Evaluările regulate ale sistemelor de securitate ajută la identificarea vulnerabilităților și la actualizarea măsurilor de protecție.

03 Măsuri de prevenire și protecție împotriva atacurilor cibernetice

Importanța conștientizării utilizatorilor despre atacurile cibernetice

- **Educația utilizatorilor este esențială.**

  Utilizatorii bine informați pot recunoaște semnele unui atac cibernetic și pot reacționa corespunzător pentru a preveni daunele.

- **Campanii de sensibilizare și instruire.**

  Implementarea campaniilor de sensibilizare ajută la educarea utilizatorilor despre riscurile cibernetice și măsurile de protecție disponibile.

- **Simulări de atacuri cibernetice.**

  Realizarea unor simulări de atacuri cibernetice ajută utilizatorii să înțeleagă cum să reacționeze în situații reale, sporind astfel securitatea.

Tehnologii și instrumente de protecție cibernetică

Utilizarea antiviruselor și software-ului de securitate.

Software-ul de securitate este crucial pentru protejarea sistemelor împotriva virușilor și atacurilor cibernetice, asigurând un mediu sigur.

Implementarea firewall-urilor eficiente.

Firewall-urile ajută la monitorizarea și controlul traficului de rețea, permițând sau blocând accesul în funcție de reguli predefinite.

Actualizări regulate ale sistemului de operare.

Menținerea sistemului de operare actualizat este esențială pentru a preveni exploatarea vulnerabilităților cunoscute de către atacatori.

Politici și proceduri de răspuns la incidente cibernetice

1

Dezvoltarea unui plan de răspuns la incidente.

Un plan bine definit de răspuns la incidente cibernetice permite organizațiilor să reacționeze rapid și eficient în fața atacurilor.

2

Formarea echipelor de răspuns la incidente.

Echipele specializate în răspunsul la incidente sunt esențiale pentru gestionarea problemelor de securitate și minimizarea impactului acestora.

3

Evaluarea și actualizarea constantă a politicilor.

Politicile de securitate trebuie revizuite și actualizate frecvent pentru a se adapta la noile amenințări cibernetice și tehnologii emergente.

04 Resurse și instrumente pentru gestionarea securității cibernetice în comunități

Importanța educației în securitatea cibernetică

Formarea continuă a personalului

Este esențial ca personalul să beneficieze de cursuri de formare continuă pentru a fi la curent cu cele mai recente amenințări cibernetice.

Campanii de conștientizare publică

Organizarea de campanii de informare care să educe cetățenii despre riscurile cibernetice și modalitățile de a se proteja.

Resurse online și ghiduri

Crearea și distribuirea de resurse online care să ofere informații clare despre cum să se protejeze în mediul digital.

Colaborarea cu experți în domeniu

Implicarea specialiștilor în securitate cibernetică pentru a oferi consultanță și sprijin comunităților în gestionarea riscurilor.

Instrumente de monitorizare a securității

Sisteme de detectare a intruziunilor

Implementarea de soluții software care monitorizează rețelele pentru a detecta activități suspecte și potențiale amenințări.

Aplicații de gestionare a parolelor

Utilizarea aplicațiilor care ajută la generarea și stocarea sigură a parolelor complex pentru a preveni accesul neautorizat.

Soluții antivirus și antimalware

Adoptarea de software antivirus actualizat care protejează sistemele împotriva virusurilor și a altor tipuri de malware.

Back-up-uri regulate ale datelor

Stabilirea unor proceduri de back-up regulate pentru a asigura recuperarea rapidă a datelor în caz de atacuri cibernetice.

Colaborarea interinstituțională

Parteneriate între instituții locale

Fostul parteneriat între diverse instituții locale pentru a îmbunătăți răspunsul la incidentele de securitate cibernetică.

Schimbul de informații

Stabilirea unor canale de comunicare eficiente pentru a facilita schimbul rapid de informații despre amenințările cibernetice.

Activități de simulare a atacurilor

Organizarea de exerciții practice care să simuleze atacuri cibernetice pentru a testa pregătirea instituțiilor implicate.

Alianțe cu sectorul privat

Formarea de alianțe cu companii din domeniul tehnologiei pentru a beneficia de expertiza și resursele acestora în securitatea cibernetică.

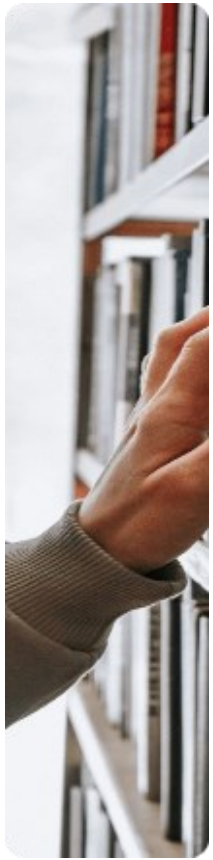
Regulamente și politici de securitate

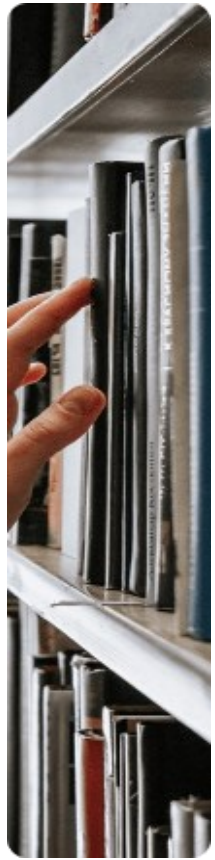
Elaborarea unor politici clare
Crearea unor politici interne bine definite care să reglementeze utilizarea tehnologiei și a datelor personale în comunități.

Norme de conformitate
Asigurarea respectării normelor legale și a reglementărilor în domeniul protecției datelor personale și a securității cibernetice.

Planuri de răspuns la incidente
Dezvoltarea unor planuri detaliate de răspuns la incidente pentru a gestiona eficient brețele de securitate și atacurile cibernetice.

Revizuirea periodică a politicilor
Implementarea unui proces de revizuire periodică a politicilor de securitate pentru a ține pasul cu evoluțiile tehnologice și amenințările emergente.





Tehnologii emergente în securitatea cibernetică

Inteligenta artificială în detecția amenințărilor

Utilizarea algoritmilor de inteligență artificială pentru a identifica rapid și eficient amenințările cibernetice emergente.

Blockchain pentru securitate

Exploatarea tehnologiei blockchain pentru a asigura integritatea și securitatea datelor în diverse aplicații comunitare.

Automatizarea răspunsului la incidente

Implementarea soluțiilor automate care pot răspunde rapid la incidentele de securitate cibernetică pentru a minimiza impactul.

Securitatea IoT

Adoptarea unor măsuri de securitate specifice pentru dispozitivele IoT care sunt din ce în ce mai utilizate în comunități.

Thank You