MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatica și Microelectronică

Departamentul Ingineria Software și Automatică

Programul de studii: Securitatea Informațională

TEMA

Importanța copiilor de rezervă și recuperarea datelor în cazul unui incident informațional

Practica Tehnologică

Student: **Chihai Adrian, SI – 211**

Coordonator întreprindere: **Bolohan Vladislav, consultant superior DTIGLE**

Coordonator universitate: **Alina Gaidarji**

Chișinău 2023

Cuprins

Introducere

Perioada și locul desfășurării practicii de la Comisia Electorală Centrală (CEC) reprezintă o oportunitate valoroasă pentru înțelegerea și aplicarea conceptelor esențiale legate de securitatea informațională și gestionarea datelor critice într-un mediu extrem de sensibil și important pentru democrație. Comisia Electorală Centrală este entitatea responsabilă cu organizarea și supravegherea procesului electoral în țara noastră și joacă un rol crucial în asigurarea transparenței și integrității alegerilor. În calitate de instituție cheie în procesul electoral, CEC gestionează și procesează o cantitate considerabilă de date sensibile și confidențiale legate de alegători, candidați și rezultatele voturilor.

Scopul acestei practici este de a înțelege și de a contribui la asigurarea securității informaționale și la eficiența proceselor de gestionare a datelor la CEC. Prin intermediul acestei practici, obiectivele propuse includ:

- Observarea și înțelegerea proceselor de gestionare a datelor și a măsurilor de securitate informațională aplicate la CEC.
- Participarea la activități practice legate de backup și recuperarea datelor în cazul unui incident informațional.
- Identificarea și documentarea procedurilor de backup existente și a protocoalelor de recuperare a datelor.
- Evaluarea relevanței și eficacității acestor proceduri în ceea ce privește menținerea continuității operaționale în timpul unui incident informațional.
- Propunerea de îmbunătățiri și recomandări pentru optimizarea strategiilor de backup și recuperare a datelor.

Această practică este deosebit de relevantă în contextul modern, în care datele sunt un activ critic pentru organizațiile din toate domeniile. Pentru Comisia Electorală Centrală, gestionarea datelor este esențială pentru buna desfășurare a procesului electoral și pentru menținerea încrederii în sistemul democratic. Un incident informațional sau o pierdere de date ar putea avea consecințe grave asupra integrității și credibilității alegerilor. Prin urmare, dezvoltarea și implementarea unui plan de backup și recuperare a datelor sunt vitale pentru asigurarea continuității operaționale în fața unor astfel de evenimente neașteptate.

În timpul acestei practici, mă aștept să dobândesc cunoștințe practice și să acumulez experiență în procesele de backup și recuperare a datelor într-un mediu critic. Provocările pot include gestionarea datelor sensibile și a resurselor limitate, precum și necesitatea de a

respecta standarde stricte de securitate informațională. De asemenea, voi fi expus la diverse scenarii potențiale de incidente informaționale și voi fi încurajat să găsesc soluții eficiente pentru a face față acestor provocări.

Prin urmare, această practică are scopul de a dezvolta competențe esențiale în securitatea informațională și gestionarea datelor, competențe care sunt extrem de valoroase în lumea tehnologică actuală și care sunt cruciale în contextul organizației CEC.

1. Importanța copiilor de rezervă din cadrul CEC-ului

Ce este un backup sau o copie de rezerva ?

Backup(copie de rezervă) - În tehnologia informației, o copie de rezervă sau procesul de copiere de rezervă se referă la copierea și arhivarea datelor de pe computer, astfel încât aceasta poate fi utilizată pentru a restabili originalul după un eveniment de pierdere a datelor. Forma de verb este de a susține în două cuvinte, în timp ce substantivul este de rezervă. Backupurile au două scopuri distincte. Scopul principal este de a recupera datele după pierderea lor, fie prin ștergerea datelor, fie prin corupere. Pierderea datelor poate fi o experiență obișnuită a utilizatorilor de calculatoare. Un sondaj din 2008 a constatat că 66% dintre respondenți au pierdut fișiere pe PC-ul lor de acasă.

Scopul secundar al copierilor de siguranță este de a recupera datele de la o dată anterioară, în conformitate cu o politică de păstrare a datelor definite de utilizator, de obicei configurată într-o aplicație de rezervă pentru cât timp sunt necesare copii ale datelor. Deși copiile de rezervă reprezintă, în mod popular, o formă simplă de recuperare în caz de catastrofe și ar trebui să facă parte dintr-un plan de recuperare în caz de dezastru, elementele de rezervă nu ar trebui să fie considerate singure ca recuperare în caz de dezastru.

Copiile de rezervă au o importanță critică pentru Comisia Electorală Centrală (CEC) și pentru oricare altă organizație care are responsabilitatea de a administra alegeri și procese electorale. Ele joacă un rol vital în asigurarea integrității și disponibilității datelor și sistemelor în timpul alegerilor, iar CEC utilizează două tipuri de backup esențiale: backupul complet și backupul offline. Iată de ce sunt acestea importante pentru CEC și pentru procesul democratic:

- **Asigură disponibilitatea datelor**: În timpul unei alegeri, este esențial ca toate datele și sistemele să fie disponibile și funcționale. Copiile de rezervă asigură că, în cazul unui eșec al sistemului principal sau al unui incident informațional, procesul electoral poate continua fără întreruperi semnificative.
- **Integritatea datelor**: Copiile de rezervă servesc ca o sursă de date autentice și intacte. Ele ajută la prevenirea pierderii sau a modificării neautorizate a datelor, ceea ce este crucial pentru asigurarea corectitudinii și transparenței alegerilor.

- **Recuperare rapidă**: În cazul unui incident sau a unui eșec al sistemului, copiile de rezervă permit CEC să recupereze rapid datele și să readucă sistemele în funcțiune. Acest lucru minimizează timpul de inactivitate și perturbările în procesul electoral.
- **Rezistența la atacuri cibernetice**: În contextul modern, alegerile pot fi vulnerabile la atacuri cibernetice. Copiile de rezervă pot fi utilizate pentru a restabili sistemele afectate de astfel de atacuri, protejând astfel integritatea și validitatea alegerilor.

Astfel, combinarea backupului complet și a backupului offline este o strategie esențială pentru CEC, asigurând protecția datelor și a sistemelor în timpul proceselor electorale, și contribuind la menținerea încrederii publicului în procesul democratic.

- **Backup complet**: Backupul complet este esențial pentru CEC deoarece furnizează o imagine integrală și actualizată a întregului mediu informatic, inclusiv a tuturor datelor și sistemelor critice utilizate în gestionarea alegerilor. Acesta poate fi utilizat pentru a restabili rapid toate sistemele în caz de eșec major sau de incident informațional care afectează infrastructura IT a CEC.
- **Backup offline**: Backupurile offline sunt stocate pe dispozitive sau medii de stocare care nu sunt conectate la rețea sau nu sunt accesibile în mod normal de la distanță. Aceasta oferă un nivel suplimentar de securitate împotriva atacurilor cibernetice, deoarece datele nu sunt expuse la rețea și sunt mai greu de compromis. Backupurile offline pot fi folosite pentru a proteja datele sensibile sau critice în cazul unui atac cibernetic.

1.1 Cum se poate pierde informația?

Statisticile arată că aproximativ 70% dintre afaceri experimentează pierderi de date. Acestea se întâmplă în fiecare zi la companiile din întreaga lume. Și atunci când nu există nicio formă de backup pentru datele corporative, acele fișiere sunt adesea pierdute pentru totdeauna.

Cum se întâmplă acest lucru? Iată câteva dintre cele mai comune cauze:

- Eroarea umană

Nimic mai puțin de 75% din pierderile de date corporative sunt cauzate de eroarea umană, conform IT Policy Compliance Group. Cea mai frecventă scenariu este ștergerea accidentală. Utilizatorii șterg involuntar e-mailuri importante, fișiere și chiar întregi foldere. Adesea, acestea le pierd din greșeală. Alteori, le șterg intenționat, fără să-și dea seama de importanța fișierelor până nu este prea târziu. Chiar și administratorii IT experimentați pot cauza pierderi de date, de exemplu, prin configurarea greșită a hardware-ului nou sau gestionarea necorespunzătoare a unei migrații de date.

- Defecțiuni hardware și software

Uneori, lucrurile pur și simplu se strică. Și atunci când se întâmplă asta, o mulțime de date pot fi distruse. Fie că este vorba despre o cădere de aplicație sau despre un disc dur de server care se defectează, datele critice pot deveni inaccesibile sau chiar corupte. Defecțiunile hardware și software sunt printre principalele cauze ale pierderii de date. Puteți reduce riscurile prin actualizarea constantă a sistemelor și înlocuirea hardware-ului vechi, dar aceste tipuri de dezastre tot vor avea loc. Singurul mod de a vă proteja cu adevărat datele este să le faceți backup în mod regulat.

- Ransomware și alte tipuri de malware

Numeroase forme de malware prezintă un risc constant pentru securitatea cibernetică. Ransomware-ul este extrem de periculos în sensul că vizează în mod specific datele dvs. De obicei, o infecție apare atunci când un utilizator deschide un atașament de e-mail infectat sau vizitează un site infectat. Ransomware-ul procedează apoi la criptarea aproape tuturor fișierelor la care poate avea acces, cerând utilizatorului să plătească o răscumpărare pentru a restabili totul la normal. Plata răscumpărării nu garantează nimic. Costurile reale apar în timpul de oprire operațională. Un raport realizat de Datto a constatat că cererea medie de răscumpărare pentru companiile mici și mijlocii a fost de 4.300 de dolari, în timp ce costul mediu al întreruperii activității a fost de 46.800 de dolari.

- Dezastre naturale

Evenimentele meteorologice extreme pot avea loc oriunde și reprezintă un risc pentru clădirile comerciale și infrastructura din interiorul lor. Incendiile și inundațiile (fie de la furtuni, fie de la ruperi de conducte) pot distruge rapid serverele locale și toate datele stocate pe acestea. În funcție de locație, afacerile se pot confrunta cu amenințarea suplimentară a dezastrelor naturale precum uraganele, tornadele și cutremurele. Pierderea unui spațiu de birouri fizic, a unui depozit sau a unei clădiri industriale poate fi devastatoare pentru o afacere. Dar dacă datele sunt șterse complet, devine și mai dificil pentru o organizație să se recupereze.

- Erori de migrație

Oricând se mută o cantitate mare de date, există riscul de pierdere a acestora. Cel mai frecvent, fișierele sunt suprascrise sau șterse accidental în timpul migrației. Acest lucru se datorează în mod obișnuit unei erori umane, dar pot exista și alți factori în joc, cum ar fi software-ul defectuos. De aceea, experții IT recomandă adesea efectuarea unui nou backup înainte de orice migrație mare (în plus față de programul obișnuit de backup). Astfel, în cazul în care datele sunt pierdute, acestea pot fi restaurate rapid din backup.

- Ștergerea malitioasă

Într-un sondaj recent realizat de Aberdeen Group, 7% dintre companii au raportat că propriii lor angajați sau contractori au distrus intenționat datele. Aceasta este în mod obișnuit un act de răzbunare atunci când un angajat este concediat din companie. Organizațiile pot reduce acest risc prin eliminarea imediată a accesului la contul lor în momentul concedierii. Cu toate acestea, singurul mod de a elimina complet riscul de

pierdere permanentă a datelor din cauza ștergerii malitioase este de a avea un sistem de backup pentru datele corporative.

1.2 Descrierea activităților de practică și observații

În lumea modernă bazată pe tehnologie, integritatea și securitatea datelor reprezintă un element esențial pentru buna desfășurare a proceselor electorale și pentru menținerea democrației. În acest context, activitățile de practică din cadrul CEC pe tema "Importanța copiilor de rezervă și recuperarea datelor în cazul unui incident informațional" au ca scop explorarea și punerea în aplicare a strategiilor și a tehnologiilor care asigură disponibilitatea și protejarea datelor critice în situații de criză. Aceste activități sunt fundamentale pentru garantarea transparenței, a corectitudinii și a continuității proceselor electorale, elemente cheie în consolidarea unui proces democratic robust și sigur. Iată activitățile pe care le-am realizat pe parcursul acestei perioade de practică

- **Analiza Infrastructurii IT existente**: Activitatea de practică începe cu o analiză cuprinzătoare a infrastructurii IT a CEC. Această etapă implică identificarea și documentarea tuturor sistemelor, datelor și resurselor critice pentru procesele electorale.
- **Evaluarea Riscurilor și Amenințărilor**: Se efectuează o evaluare a riscurilor și amenințărilor potențiale care pot afecta integritatea și disponibilitatea datelor și sistemelor. Această etapă ajută la identificarea scenariilor de incidente informaționale pe care CEC ar putea să le întâmpine.
- **Planificarea Strategiei de Backup**: Pe baza riscurilor identificate, se dezvoltă o strategie de backup care definește tipurile de date care trebuie să fie copiate de rezervă, frecvența efectuării backup-urilor și metodele de stocare a acestora.
- **Testarea Periodică a Backup-urilor**: Se efectuează teste regulate de către personal în care am fost implicat și eu pentru a verifica eficacitatea copiilor de rezervă și a procedurilor de recuperare a datelor. Aceasta implică restaurarea datelor din backup-uri pentru a asigura că acestea pot fi recuperate cu succes în caz de necesitate.
- **Simularea Incidentelor Informaționale**: Personalul CEC participă la simulări de incidente informaționale pentru a evalua modul în care ar reacționa în cazul unui atac cibernetic sau al unui incident similar. Acest lucru ajută la dezvoltarea capacității de recuperare în timp real.
- **Recuperarea datelor în timp real**: În cadrul exercițiului practic, personalul CEC va fi pus în situații reale pentru a implementa procedurile de recuperare a datelor în timp real. Acest lucru va implica restaurarea rapidă a datelor critice și a sistemelor afectate pentru a minimiza impactul asupra desfășurării corecte a proceselor electorale.
- **Educația și Conștientizarea Personalului**: Activitatea de practică include și o componentă de educație și conștientizare pentru personal, pentru a-i învăța despre importanța copiilor de rezervă și a securității datelor în general.

În urma realizării acestor activitați am obținut noi cunoștințe și realizat anumite observații care sunt foarte importante pentru acest tip de activitate ca și backupul, securizarea și recuperarea datelor în cazul unor atacuri informatice.

Rezultate:

- **Înțelegerea Profundă a Importanței Copiilor de Rezervă:** Unul dintre rezultatele cheie ale practicii a fost dobândirea unei înțelegeri profunde a importanței critice a copiilor de rezervă în contextul proceselor electorale. Am înțeles că aceste copii de siguranță reprezintă o măsură esențială pentru asigurarea continuității și integrității alegerilor.

- **Competențe Tehnice Dezvoltate:** Prin participarea la activități de practică, am dezvoltat competențe tehnice în ceea ce privește crearea, gestionarea și restaurarea copiilor de rezervă. Am învățat să utilizez diferite soluții și tehnologii pentru a proteja datele și pentru a le readuce în funcțiune în caz de incident.

- **Experiență în Simularea Incidentelor:** Am avut oportunitatea de a participa la simulări de incidente informaționale, ceea ce m-a ajutat să înțeleg cum să reacționez și să gestionez eficient situații de criză legate de date și securitatea informațională.

- **Asigurarea Conformității cu Reglementările**: Am înțeles că CEC are responsabilitatea de a respecta reglementările și standardele legale privind protecția datelor și securitatea cibernetică în cadrul proceselor electorale. Această conformitate este crucială pentru a evita posibilele consecințe juridice și pentru a menține integritatea alegerilor.

Observații

- **Complexitatea Gestionării Backup-urilor:** Un aspect observat a fost complexitatea gestionării backup-urilor într-un mediu complex, cum este cel al unei instituții precum CEC. Planificarea, implementarea și menținerea unor soluții de backup eficiente necesită resurse și expertiză considerabile.

- **Importanța Educației Continuă:** Am observat că educația continuă este esențială pentru personalul CEC în ceea ce privește aspectele legate de securitatea cibernetică și procedurile de recuperare a datelor. Formarea constantă este crucială pentru a rămâne la curent cu noile amenințări și tehnologii.

- **Responsabilitatea Crescută:** Practica la CEC mi-a arătat cât de mare este responsabilitatea unei instituții în asigurarea integrității proceselor electorale. Protejarea datelor și a sistemelor este un angajament critic pentru a asigura corectitudinea și transparența alegerilor.

- **Sensibilizarea la Securitatea Informațională:** Practica a subliniat nevoia de a crește nivelul de conștientizare a tuturor angajaților CEC cu privire la practicile de securitate informațională. Fiecare membru al organizației joacă un rol în protejarea datelor și trebuie să fie educat în acest sens.
- **Amenințări Evolutive:** Am observat că amenințările cibernetice evoluează rapid și devin tot mai sofisticate. Astfel, este esențial să existe o abordare dinamică și actualizată pentru protecția datelor, care să țină pasul cu aceste amenințări în continuă schimbare.

- **Rapiditatea Recuperării:** Observația că rapiditatea cu care datele și sistemele pot fi recuperate în caz de incident poate face diferența între un impact minor și unul major. Procedurile de recuperare eficiente sunt cruciale pentru minimizarea timpului de inactivitate.
- **Amenințări Evolutive:** Am observat că amenințările cibernetice evoluează rapid și devin tot mai sofisticate. Astfel, este esențial să existe o abordare dinamică și actualizată pentru protecția datelor, care să țină pasul cu aceste amenințări în continuă schimbare.

1.3 Analiza și concluzii parțiale

Stagiul de practică la Comisia Electorală Centrală (CEC) focusat pe importanța copiilor de rezervă și recuperarea datelor în cazul unui incident informațional a fost o experiență deosebit de valoroasă și învățătoare.

Pe parcusul acestei luni am dezvoltat noi cunoștințe în domeniul tehnic în domeniul securității informționale și a procedurii de salvare și recuperare a datelor. Participând și realizând testele de recuperare a datelor am înțeles cum trebuie configurate și gestionate aceste date cât mai eficient. Acest proces de realizare a copiilor de rezervă este unul foarte critic care asigură diponibilitatea și protejarea datelor în fața amenințărilor pe care le putem întâlni oriunde mereu în mediul online. Pentru o siguranță continuă în acest mediu instituțional, planificare, implementarea și menținerea soluțiilor de backup este necesar să se investească în aceste resurse și sa fie verificate pentru a fi capabile si funcționale.

În cadrul acestei instituții sunt impuse niște reguli care trebuie respecate pentru a preveni cele mai groaznice scenarii, iată câteva reguli care trebuie respectate și realizate de angajații competenți sau sunt realizate de un sistem automat.

1.3.1 Cum sunt gestionate copiile de rezerva pentru baza de date

Procedurile de backup pentru bazele de date trebuie să fie concepute astfel încât să permită restaurarea datelor din bazele de date din cadrul sistemului informațional al CEC.

Acest lucru trebuie să se facă în concordanță cu indicatorii de performanță stabiliți pentru fiecare serviciu de bază de date în parte. Această restaurare a datelor trebuie să fie posibilă în următoarele situații:

- în cazul defecţiunilor tehnice la nivelul componentelor hard aferente serviciilor de gestiune a BD;
- în cazul erorilor logice la nivelul softului de sistem sau a softului aplicativ;
- în cazul eliminărilor / modificărilor nesancţionate, deliberate sau accidentale ale datelor din BD;
- în cazul modificărilor eronate în setările şi configuraţia serviciului de gestiune a BD;

Pentru toate bazele de date (BD), este esențial să se efectueze zilnic copii de rezervă diferențiale, asigurând astfel că se capturează modificările recente ale datelor. Săptămânal, trebuie realizate copii de rezervă depline pentru a garanta că toate datele sunt complet salvate. Copiile de rezervă vor fi păstrate sub formă de fișiere arhivate pe suporturi de stocare, cum ar fi benzi magnetice sau unități de hard disk extern, care vor fi ținute într-o cameră special destinată serverelor. Se va menține un istoric al ultimelor 5 copii de rezervă, permițând recuperarea datelor în diferite puncte temporale.

În cazul bazelor de date critice, se recomandă utilizarea tehnicii de replicare a datelor. Aceasta implică crearea unei copii a bazei de date pe un alt server sau locație geografică, asigurând astfel o redundantă a datelor și o recuperare rapidă în caz de eșec al serverului principal sau al mediului de stocare. Replicarea datelor este o măsură suplimentară de securitate pentru a proteja informațiile sensibile și pentru a minimiza timpul de inactivitate în caz de probleme cu serverul principal.

1.3.2 Cum sunt gestionate copiile de rezerva pentru fișiere și documente electronice

Pentru datele și informația stocate sub formă de documente electronice, este necesar să se efectueze copii de rezervă regulate. Acest lucru are ca scop asigurarea capacității de a restaura informația în următoarele situații:

- în cazul defecţiunilor tehnice la nivelul componentelor hard;
- în cazul erorilor logice la nivelul softului de sistem;
- în cazul eliminărilor / modificărilor nesancţionate, deliberate sau accidentale ale informaţiei;

Toate documentele şi fişierele de lucru ale utilizatorilor, trebuie să fie păstrate pe serverul de fişiere al CEC. Pentru informaţia de pe serverul de fişiere se vor face regulat copii de rezervă, precum urmează:

- copii depline săptămânal. Vor fi menţinute ultimele 2 copii depline;
- copii diferenţial L/M/Mi/J. Vor fi menţinute ultimele 5 copii depline;

1.3.3 Cum sunt gestionate copiile de rezerva pentru sistem server

Sistemele server reprezintă mediile de funcționare și software-ul fundamental instalat pe acestea, care garantează că serviciile și aplicațiile sunt disponibile și rulează corespunzător. Este esențial să se efectueze copii de siguranță ale acestor sisteme pentru a asigura posibilitatea de a restaura acele sisteme pe o altă infrastructură hardware (în cazul în care apar probleme tehnice) sau pe aceeași infrastructură (în cazul apariției erorilor logice la nivelul sistemului de operare sau a software-ului de sistem instalat).

Copii de rezervă pentru sistemele server se vor efectua la nivelul serviciilor instalate (unde este posibil acest lucru) şi la nivelul sistemului în întregime.

Frecvenţa copiilor de rezervă este de cel puţin o dată în săptămână, sau la efectuarea modificărilor semnificative.

1.3.4 Cum sunt gestionate copiile de rezerva pentru echipamentele de rețea

Fișierele de configurare pentru dispozitivele de rețea trebuie să fie păstrate într-un mediu sigur pentru a permite revenirea la setările anterioare în caz de necesitate. Aceste reguli pentru efectuarea copiilor de siguranță a fișierelor de configurare pe dispozitivele de rețea sunt aplicabile în general tuturor dispozitivelor de rețea și includ următoarele aspecte:

- O copie backup a fişierului de configuraţie se face înainte de orice modificare pe echipamentul de reţea.
- O copie backup a fişierului de configuraţie se face imediat după efectuarea modificărilor în configuraţia echipamentelor de reţea.
- Copiile backup pentru configuraţiile echipamentelor de reţea sunt păstrate pentru o perioadă de minim 3 ani;
- Copiile backup pentru configuraţiile echipamentelor de reţea sunt păstrate într-o mapă dedicată pe serverul de fişiere. La mapa respectivă au acces doar responsabilii din cadrul DTIGLE. Pentru fiecare echipament de reţea este creată o mapă dedicată, numele căreia coincide cu identificatorul echipamentului de rețea. Mapa respectivă este inclusă în backup-ul serverului de fişiere

1.3.5 Menținerea copiilor de rezervă într-un loc extern (offsite).

Pentru toate datele şi informaţia importantă din cadrul sistemului informaţional al CEC este necesară deţinerea unei copii de rezervă în afara sediului de Bază.

Siguranța datelor din copiile de rezervă este de o importanță crucială, deoarece acestea conțin informații sensibile și confidențiale. Prin urmare, accesul la aceste copii de rezervă trebuie să fie stricte controlat și permis doar personalului responsabil din cadrul DTIGLE, în conformitate cu atribuțiile lor. Orice transfer sau stocare a acestor copii de rezervă în afara sediului principal al CEC trebuie să fie efectuat folosind metode de criptare pentru a asigura securitatea și confidențialitatea datelor.

1.3.6 Testarea copiilor de rezervă

Pentru a asigura că copiile de rezervă sunt complete și pot fi utilizate în situații de urgență, este necesar să se efectueze teste periodice asupra acestora. Acest lucru poate fi realizat prin utilizarea copiilor de rezervă în diverse contexte, cum ar fi crearea de medii de test sau dezvoltare sau în alte situații în care este necesar să se restaureze datele. În plus, dacă CEC are la dispoziție tehnologii la nivel de hardware sau utilitare de sistem care permit verificarea integrității copiilor de rezervă, aceste tehnologii trebuie utilizate în mod obligatoriu, cum ar fi folosirea funcției "RESTORE VERIFYONLY" pentru bazele de date MS SQL, pentru a confirma că copiile de rezervă sunt corecte și utilizabile.

1.3.7 Gestionarea sigura a copiilor de rezervă și recuperarea datelor la CEC

- Experiența de stagiu la Comisia Electorală Centrală (CEC) a evidențiat importanța gestionării adecvate a copiilor de rezervă și a recuperării datelor într-un mediu instituțional. Această practică a relevat că procedurile de backup și restaurare sunt esențiale pentru asigurarea disponibilității și securității datelor în fața amenințărilor cibernetice și a altor incidente.

- Pentru a asigura integritatea și disponibilitatea datelor, CEC a implementat reguli clare și proceduri pentru gestionarea copiilor de rezervă în diferitele sale medii, cum ar fi bazele de date, fișierele electronice, sistemele server și echipamentele de rețea. Aceste reguli includ frecvența copiilor de rezervă, păstrarea acestora pe suporturi de stocare securizate și testarea periodică a copiilor de rezervă pentru a se asigura că acestea sunt funcționale.

- Pentru o securitate sporită, CEC a adoptat practici de stocare a copiilor de rezervă în locații externe (offsite) și utilizează tehnologii de criptare pentru protejarea acestora. Testarea regulată a copiilor de rezervă și verificarea integrității acestora sunt procese esențiale pentru a se asigura că datele pot fi restaurate eficient în caz de necesitate. Astfel, CEC demonstrează angajamentul său față de securitatea și continuitatea operațiunilor în mediul său instituțional.

2 Evaluarea procesului de backup si prevenire a pierderii informațiilor

Evaluarea procesului de prevenire a pierderii datelor la Comisia Electorală Centrală (CEC) nu reprezintă doar o formalitate, ci o componentă esențială a responsabilităților instituției într-un peisaj informațional în continuă schimbare. Într-o eră în care datele devin din ce în ce mai valoroase și vulnerabilitatea la amenințările cibernetice este în creștere constantă, CEC înțelege că securitatea și disponibilitatea informațiilor sunt esențiale pentru buna

desfășurare a proceselor electorale și a misiunii sale de a asigura un proces democratic și transparent.

Protecția datelor sensibile și a informațiilor referitoare la alegeri nu este doar o obligație legală, ci și o necesitate strategică pentru CEC. Procesul electoral implică gestionarea unor volume masive de date, inclusiv date personale ale alegătorilor, rezultatele votului și informații critice pentru funcționarea corectă a democrației. Orice incident care duce la pierderea sau compromiterea acestor date ar putea avea consecințe serioase asupra integrității procesului electoral și a încrederii publice în acesta.

2.1 Protejarea și Gestionarea Eficientă a Datelor Sensibile la CEC

Procesul de prevenire a pierderii datelor la Comisia Electorală Centrală (CEC), așa cum este descris în informațiile furnizate, pare să fie bine structurat și să pună accent pe securitatea și disponibilitatea datelor. Cu toate acestea, pentru o evaluare completă, ar trebui luate în considerare mai multe aspecte:

- **Gestionarea copiilor de rezervă:** Procesul de realizare a copiilor de rezervă pentru bazele de date, fișierele electronice, sistemele server și echipamentele de rețea este detaliat și corect planificat. Este important ca copiile de rezervă să fie efectuate în mod regulat, iar procedurile să fie respectate cu strictețe pentru a asigura că datele pot fi restaurate eficient în caz de necesitate.
- **Securitatea datelor:** Folosirea criptării pentru transmiterea și stocarea copiilor de rezervă în afara sediului principal al CEC reprezintă o măsură importantă pentru protejarea datelor confidențiale. Controlul strict al accesului la copiile de rezervă și menținerea unui istoric al acestora contribuie, de asemenea, la securitatea datelor.
- **Testarea și verificarea copiilor de rezervă:** Procesul de testare periodică a copiilor de rezervă și verificarea integrității acestora sunt esențiale pentru asigurarea funcționalității acestora. Utilizarea tehnologiilor de verificare a integrității datelor, cum ar fi "RESTORE VERIFYONLY" pentru bazele de date MS SQL, este o practică bună.
- **Gestionarea echipamentelor de rețea:** Regulile privind păstrarea copiilor de rezervă pentru fișierele de configurare ale echipamentelor de rețea și crearea de copii de siguranță înainte și după modificări sunt proceduri importante pentru a asigura disponibilitatea rețelei în caz de necesitate.
- **Stocarea offsite:** Păstrarea unor copii de rezervă în afara sediului principal al CEC contribuie la protejarea datelor în caz de dezastre naturale sau alte evenimente care pot afecta sediul central.

În ansamblu, procesul de prevenire a pierderii datelor pare să fie bine gândit și implementat la CEC, cu un accent adecvat pe securitate și disponibilitate. Cu toate acestea, este important ca instituția să continue să supravegheze și să actualizeze aceste procese în funcție de evoluțiile tehnologice și amenințările cibernetice în continuă schimbare pentru a asigura protecția datelor pe termen lung.

3 Diversificarea Metodelor de Backup

Un aspect deosebit de important în cadrul Comisiei Electorale Centrale (CEC) este diversificarea metodelor de backup. Această diversitate constă în utilizarea atât a backup-urilor complete, cât și a celor offline. În continuare, vom explora de ce este esențial să avem ambele metode în arsenalul nostru de protecție a datelor.

Backup Complet - Protecția Integrală

Un backup complet reprezintă o copie a întregului set de date și informații la un moment dat. Această metodă oferă cea mai înaltă grad de protecție, deoarece orice componentă sau fișier din sistem este inclus în backup. În cazul unui incident, precum o defecțiune hardware majoră sau o pierdere a datelor, un backup complet permite restaurarea rapidă a întregului mediu la starea sa inițială. Pentru CEC, aceasta înseamnă că datele vitale legate de procesele electorale și de gestionarea informațiilor electorale sunt protejate integral.

Backup Offline - Protecția împotriva Amenințărilor Cibernetice

Într-o lume în care amenințările cibernetice devin tot mai sofisticate, backup-urile offline devin un scut suplimentar de apărare. Acest tip de backup implică stocarea datelor într-un mediu izolat de rețeaua online. Prin această abordare, se minimizează riscul ca atacatorii cibernetici să aibă acces la copiile de rezervă și să le corupă sau să le șteargă. Astfel, chiar și în cazul unui atac cibernetic, datele pot fi recuperate din backup-urile offline, asigurând astfel continuitatea proceselor electorale și integritatea datelor electorale.

În acest capitol, vom explora în detaliu implementarea și gestionarea acestor două metode de backup cruciale la CEC. Vom evidenția beneficiile și provocările fiecărei abordări și vom arăta cum acestea lucrează împreună pentru a asigura securitatea și disponibilitatea datelor în fața unei game diverse de amenințări.

3.1 Procesul de Backup Complet la CEC

Backup-ul complet reprezintă un proces crucial în cadrul Comisiei Electorale Centrale (CEC) pentru protejarea și asigurarea disponibilității datelor critice legate de procesele electorale și gestionarea informațiilor electorale. Acesta presupune realizarea unei copii exacte și integrale a tuturor datelor și informațiilor existente într-un moment dat. Iată cum funcționează acest proces în cadrul CEC:

- **Identificarea Surselor de Date:** CEC identifică toate sursele de date și informații critice care trebuie să fie incluse în backup-ul complet. Acestea pot include baze de date cu informații electorale, date despre candidați, date de vot, procese electorale, precum și orice altă informație relevantă pentru funcționarea instituției.

- **Inițierea Procesului de Backup:** Un program sau o soluție software de backup este utilizat pentru a iniția procesul. Acesta poate fi configurat pentru a rula în mod regulat, de exemplu, săptămânal sau lunar, în funcție de politica de backup a CEC.

- **Captarea Datelor:** Datele din sursele identificate sunt citite și copiate într-un loc de stocare specificat. De obicei, aceasta implică realizarea unui "snapshot" al datelor, asigurându-se că toate fișierele și structurile de date sunt incluse.

- **Compresia Datelor (opțională):** În unele cazuri, datele pot fi comprimate înainte de a fi stocate. Acest lucru reduce cerințele de spațiu de stocare, dar poate prelungi timpul necesar pentru backup și restaurare.

- **Criptarea Datelor:** Pentru a asigura securitatea datelor, acestea pot fi criptate înainte de stocare. Aceasta previne accesul neautorizat la datele din backup.

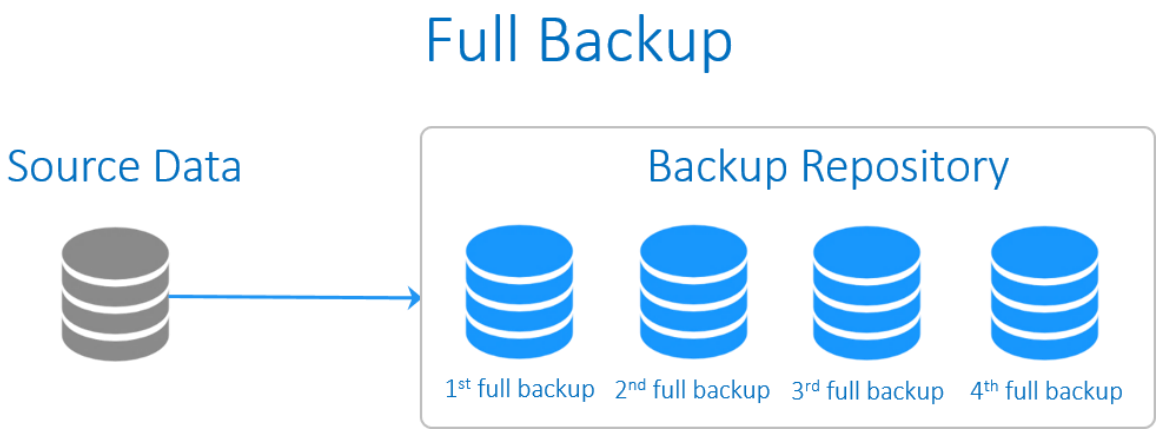
- **Salvarea în Locația de Backup:** Datele copiate sunt stocate într-o locație de backup dedicată, cum ar fi un server de backup sau discuri externe securizate. Acesta poate fi un spațiu de stocare fizic sau cloud storage, în funcție de politica de stocare a datelor a CEC.

- **Politica de Retenție:** CEC stabilește o politică de retenție care determină cât timp trebuie păstrate backup-urile complete. Aceasta poate varia în funcție de tipul de date și de cerințele legale sau organizaționale.

- **Restaurarea Datelor:** În caz de necesitate, datele pot fi restaurate dintr-un backup complet. Acest lucru se realizează de obicei prin selectarea setului de backup dorit și prin procesul de restaurare adecvat.

Exemplu de utilizare: Dacă în timpul unui scrutin electoral apar probleme tehnice sau se pierd date critice, CEC poate utiliza un backup complet pentru a restaura rapid și eficient toate datele la starea lor inițială. Acest lucru asigură integritatea și disponibilitatea datelor electorale în timp real, garantând transparența și corectitudinea procesului electoral.

Figura 3.1.1 Schema Backupului Complet



3.2 Procesul de Backup Offline la CEC

Un aspect esențial al strategiei de backup la Comisia Electorală Centrală (CEC) implică utilizarea backup-urilor offline. Această metodă asigură o protecție suplimentară pentru datele și informațiile deosebit de sensibile gestionate de instituție.

Cum Funcționează Backupul Offline:

Backupul offline implică stocarea datelor și informațiilor într-un mediu izolat de rețeaua online și de sistemele în funcțiune. Această separare fizică este crucială pentru a proteja datele împotriva amenințărilor cibernetice, cum ar fi malware-ul, ransomware-ul sau atacurile de tip phishing, care pot viza stocarea online a datelor. Iată cum funcționează acest proces în cadrul CEC:

- **Generarea Copiilor de Rezervă Offline:** La CEC, datele sensibile și vitale pentru procesele electorale și administrarea acestora sunt copiate periodic și create copii de rezervă offline. Acest proces poate implica utilizarea discurilor dure externe, a unităților de stocare offline sau chiar a suporturilor fizice, cum ar fi DVD-uri sau benzi magnetice.

- **Fizic și Logic Izolat:** Copiile de rezervă offline sunt ținute într-un mediu fizic izolat de rețeaua online și de alte sisteme. Aceasta poate însemna depozitarea lor într-o cameră specială cu acces restricționat sau într-un loc securizat la distanță de sediul central al CEC.

- **Acces Strict Controlat:** Doar personalul autorizat și responsabil din cadrul CEC are acces la aceste copii de rezervă offline. Acest acces este stricte controlat și monitorizat pentru a preveni orice potențială amenințare internă.

- **Recuperare în Caz de Urgență:** Backupurile offline sunt menținute pentru a asigura continuitatea operațiunilor în caz de necesitate. Dacă datele sunt compromise sau pierdute din cauza unui eveniment neașteptat, cum ar fi un atac cibernetic sau un defect major al sistemului, aceste copii de rezervă offline pot fi utilizate pentru a restaura datele la starea lor inițială.

Exemple de Situații de Utilizare a Backup-urilor Offline la CEC:

- **Recuperare După un Atac Cibernetic:** Dacă CEC ar fi ținta unui atac cibernetic care ar compromite datele stocate online, copiile de rezervă offline pot fi utilizate pentru a restabili datele afectate.

- **Protecția împotriva Ransomware-ului:** Ransomware-ul poate cripta datele stocate online și cere răscumpărarea pentru decriptarea lor. Cu backup-urile offline, CEC poate ignora astfel de cereri și restaura datele din copii de rezervă sigure.

- **Recuperare După Defecțiuni Hardware Majore:** În cazul unor defecte hardware majore sau pierderi de date, copiile offline pot fi utilizate pentru a restabili funcționalitatea rapidă a sistemelor critice.

  Backupurile offline reprezintă o parte crucială a strategiei de securitate și continuitate la CEC, asigurând că datele sensibile și procesele electorale pot continua să funcționeze în ciuda amenințărilor cibernetice sau a altor evenimente neașteptate. Această abordare oferă un strat suplimentar de protecție pentru datele vitale ale instituției.

3.3 Compararea Avantajelor și Dezavantajelor Backupului Complet și a Celui Offline

Backup Complet

Avantaje:

- **Protecție Integrală:** Backupul complet include toate datele și informațiile, asigurând o protecție cuprinzătoare împotriva pierderii datelor.
- **Restaurare Rapidă:** În caz de necesitate, datele pot fi restaurate rapid la starea lor inițială, asigurând continuitatea operațiunilor.
- **Gestionare Ușoară:** Backupul complet este adesea mai ușor de gestionat și de implementat, deoarece include toate datele într-o singură copie.

Dezavantaje:

- **Spatiu de Stocare Mare:** Backupurile complete pot necesita o cantitate semnificativă de spațiu de stocare, ceea ce poate crește costurile asociate cu infrastructura de backup.
- **Timp de Backup Mai Lung:** Realizarea unui backup complet poate dura mai mult timp în comparație cu alte metode, ceea ce poate afecta disponibilitatea datelor în timpul procesului de backup.

Backup Offline

Avantaje:

- **Protecție Suplimentară:** Backupurile offline oferă o protecție suplimentară împotriva amenințărilor cibernetice, deoarece datele sunt izolate de rețeaua online.
- **Rezistență la Ransomware:** Datorită izolării, backupurile offline sunt rezistente la ransomware și alte forme de malware care vizează datele online.
- **Confidențialitate Îmbunătățită:** Datele offline sunt mai greu accesibile pentru persoane neautorizate, ceea ce îmbunătățește confidențialitatea informațiilor.

Dezavantaje:

- **Acces Fizic Necesar:** Pentru a restaura datele din backupurile offline, este necesar accesul fizic la discurile sau mediile de stocare offline, ceea ce poate fi dificil în anumite situații.
- **Complexitate Suplimentară:** Gestionarea și menținerea backupurilor offline pot adăuga complexitate procesului de backup și pot necesita măsuri de securitate suplimentare pentru protecția mediilor offline.

În rezumat, backupul complet și cel offline îndeplinesc funcții specifice și prezintă avantaje distincte. Atunci când sunt utilizate în mod corespunzător și integrate eficient, aceste două metode pot oferi o protecție solidă și cuprinzătoare pentru datele unei organizații, asigurându-le securitatea în fața unei game variate de amenințări.

Observații

Stagiul meu de practică la Comisia Electorală Centrală (CEC) a fost o experiență excepțională și formativă. Pe parcursul acestui stagiu, am avut ocazia să observ și să învăț o serie de aspecte semnificative despre modul în care CEC gestionează și protejează datele critice și sensibile legate de procesele electorale. Iată câteva observații și feedback-uri pozitive:

- **Dedicare față de Securitatea Datelor**: Una dintre cele mai notabile caracteristici ale CEC este angajamentul lor ferm față de securitatea datelor. Procedurile și politici bine planificate pentru gestionarea copiilor de rezervă, securitatea datelor și stocarea offline sunt semnificative și demonstrează conștientizarea instituției cu privire la importanța protejării informațiilor critice.

- **Abordare Profesională**: Echipa CEC se caracterizează prin profesionalism și atenție la detalii. Fiecare aspect al procesului de gestionare a datelor este abordat cu seriozitate și responsabilitate. Aceasta este o practică excelentă în asigurarea corectitudinii și integrității proceselor electorale.

- **Diversificarea Metodelor de Backup**: Am observat cu satisfacție utilizarea atât a backupului complet, cât și a celui offline pentru protejarea datelor. Această abordare diversificată adaugă un nivel suplimentar de siguranță și este un exemplu de bună practică în domeniul securității datelor.

- **Colaborarea și Echipa Unită**: Stagiul meu a implicat colaborarea cu profesioniști dedicati și cu o echipă unită la CEC. Acest lucru a fost esențial pentru înțelegerea practicilor și pentru dezvoltarea abilităților în gestionarea datelor și securitatea informațională.

- **Oportunitate de Învățare**: CEC a oferit oportunități excelente de învățare și dezvoltare. Faptul că am putut contribui la evaluarea și analiza strategiilor de securitate a datelor a fost o experiență de neuitat și m-a ajutat să aplic cunoștințele teoretice într-un context real.

Feedback-ul pozitiv și observațiile mele reflectă angajamentul și profesionalismul CEC în gestionarea datelor și securitatea informațională. Această experiență va rămâne o bază solidă pentru cariera mea viitoare și pentru contribuția mea la domeniul securității datelor. Sunt recunoscător pentru această oportunitate și sunt convins că CEC va continua să fie un model de excelență în acest domeniu important.

Concluzie

În cadrul Comisiei Electorale Centrale (CEC), strategiile de prevenire a pierderii datelor au fost elaborate și implementate cu atenție și dedicație. Prin detaliile tehnice și procesele bine planificate pentru gestionarea copiilor de rezervă, securitatea datelor, testarea și verificarea acestora, precum și stocarea offline, CEC a demonstrat angajamentul față de protejarea datelor vitale și sensibile.

Folosind backupuri complete pentru bazele de date, fișierele electronice, sistemele server și echipamentele de rețea, CEC și-a asigurat capacitatea de a restaura datele rapid în caz de necesitate. Utilizarea backupurilor offline adaugă un strat suplimentar de securitate, izolând datele de amenințările cibernetice și alte riscuri potențiale.

Într-o lume în care pierderea de date este o realitate pentru multe organizații, CEC a făcut un pas important pentru a se asigura că informațiile esențiale pentru procesele electorale și funcționarea instituției sunt protejate și disponibile în orice moment. Abordarea lor atent planificată și implementată cu precizie serveste ca exemplu de bună practică în gestionarea datelor în mediul instiuțional.

Cu toate acestea, este important de subliniat că amenințările cibernetice și tehnologia evoluează în mod constant. Prin urmare, CEC trebuie să rămână vigilentă și să actualizeze în mod regulat strategiile și tehnologiile de protecție a datelor pentru a se adapta la aceste schimbări în curs. Prin continuarea angajamentului lor față de securitatea datelor, CEC poate asigura protecția pe termen lung a informațiilor critice și contribuie la integritatea și transparența proceselor electorale.

În concluzie, angajamentul continuu față de securitatea datelor și adaptabilitatea la schimbările tehnologice și amenințările cibernetice sunt esențiale pentru menținerea integrității și disponibilității datelor în cadrul Comisiei Electorale Centrale. Cu această abordare proactivă și cu măsurile deja implementate, CEC poate aborda cu încredere provocările din ce în ce mai complexe ale gestionării datelor în mediul instituțional și poate contribui la consolidarea democrației prin asigurarea corectitudinii proceselor electorale.

Prin urmare, prin concentrarea asupra dezvoltării continue a strategiilor și măsurilor de protecție a datelor, CEC poate să continue să fie un model de excelență în gestionarea datelor și să asigure integritatea proceselor electorale în viitorul său.

Cu siguranță, ca viitor specialist în domeniul securității informaționale și al gestionării datelor, această experiență de stagiu la Comisia Electorală Centrală (CEC) a fost extrem de valoroasă pentru dezvoltarea mea profesională. Am avut oportunitatea de a aplica cunoștințele teoretice într-un mediu real, lucru care m-a ajutat să înțeleg mai bine complexitatea și importanța măsurilor de securitate a datelor în instituții critice.

Prin implicarea în procesul de evaluare și dezvoltare a strategiilor de prevenire a pierderii datelor la CEC, am acumulat cunoștințe practice despre proceduri de backup, securitatea datelor și testarea

integrității acestora. Această experiență m-a pregătit pentru a deveni un profesionist mai bine pregătit pentru a face față amenințărilor cibernetice și pentru a contribui la protejarea datelor organizațiilor în viitor.

De asemenea, am învățat importanța colaborării cu colegii și experții din domeniu pentru a găsi soluții eficiente la provocările legate de securitatea datelor. Această abilitate de colaborare și cunoștințele acumulate sunt extrem de valoroase pentru cariera mea viitoare.

În concluzie, această experiență la CEC m-a ajutat să înțeleg mai bine complexitatea gestionării datelor și securității informaționale, iar cunoștințele și abilitățile dobândite în timpul stagiuului vor juca un rol crucial în viitorul meu ca specialist în acest domeniu.