Universitatea Tehnică a Moldovei

TEMA: SECURITATEA BAZEI DE DATE A FEDERAȚIEI NAȚIONALE DE TAEKWON-DO

Student: **Covali Nicolae**

Cordonator: **conf, univ., dr. Tîrșu Valentina**

Chişinău, 2023

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică şi Telecomunicaţii

Departamentul Telecomunicaţii Şi Sisteme Electronice

Admis la susţinere

Şef departament:
Sava Lilia conf. univ., dr.

_____

„ _" 2023

TEMA: SECURITATEA BAZEI DE DATE A FEDERAȚIEI NAȚIONALE DE TAEKWON-DO

Teză de master

Student: **Covali Nicolae MMRT-211M**

Coordonator: **Tîrşu Valentina conf.univ.,dr.**

Consultant: **Sava Lilia conf. univ., dr.**

Chişinău, 2023

ADNOTARE

Covali Nicolae, studentului grupei MMRT-211M

Tema.SECURITATEA BAZEI DE DATE A FEDERAȚIEI NAȚIONALE DE TAEKWON-DO

Cuvinte cheie: VPN, LAN, IP , WAN, rețea, NAT, Criptare, securitate, bază de date;

Scopul lucrării este de a asigurarea o bună securitate a bazelor de date a tuturor filialelor din cadrul Federațiein Naționale de Taekwon-do și pentru a asigura securitatea transportului de date în cadrul reţelei de comunicare.

Lucrarea de faţă se axează pe următoarele obiective:

Implementării unei rețele private în cadrul unei instituții

Asigurarea siguranței transportului de date

Implementarea soluțiilor de modernizare a rețelei de comunicații virtuale

Examinarea tehnologiilor şi diverselor metode pentru a asigura o bună protecție a bazelor de date.

Disponibilitate: Asigurarea disponibilității bazei de date pentru utilizatori și aplicații, astfel încât să poată fi accesată și utilizată în orice moment.

Integritate: Asigurarea integrității informațiilor din baza de date, astfel încât să fie precisă și fiabilă.

Siguranță: Asigurarea protecției împotriva accesului neautorizat sau a modificărilor nedorite la informațiile din baza de date.

Performanță: Asigurarea unei performanțe adecvate a bazei de date pentru a satisface nevoile de acces și utilizare ale utilizatorilor și aplicațiilor.

Scalabilitate: Asigurarea capacității bazei de date de a se extinde și de a face față creșterii volumului de informații și a cererilor de acces.

Conformitate: Respectarea regulilor și standardelor aplicabile în domeniul bazelor de date, cum ar fi reglementările privind protecția datelor personale și guvernamentale

Semnificația și valoare aplicativă constă în:

Proiectarea rețelei pentru asigurarea securității bazelor de date a Federaţiei Naţionale de Taekwon-do și pentru a asigura securitatea transportului de date în cadrul reţelei de comunicare prin implimentarea practică conform materialelor prezentate în capitole. Au fost descrise deciziile și tehnicile de bază utilizate în perioada proiectării și metodele de cercetare care au condus la acestea.

Această lucrare oferă o amplă analiză și recomandări pentru a asigura o bună securitate a bazelor de date.

ANNOTATION

Covali Nicolae, student of the MMRT-211M group

Theme. NATIONAL TAEKWON-DO FEDERATION DATABASE SECURITY

Keywords: VPN, LAN, IP, WAN, network, NAT, Encryption, security, database;

The aim of the work is to ensure a good security of the databases of all branches within the National Taekwon-do Federation and to ensure the security of data transport within the communication network.
The present work focuses on the following objectives:
Implementation of a private network within an institution
Ensuring the safety of data transport
Implementation of virtual communication network modernization solutions
Examining technologies and various methods to ensure good database protection.
Availability: Making the database available to users and applications so that it can be accessed and used at any time.
Integrity: Ensuring the integrity of the information in the database so that it is accurate and reliable.
Security: Ensuring protection against unauthorized access or unwanted changes to database information.
Performance: Ensuring adequate database performance to meet user and application access and usage needs.
Scalability: Ensuring the ability of the database to expand and cope with the increase in the volume of information and access requests.
Compliance: Complying with applicable database rules and standards, such as government and personal data protection regulations

The meaning and applicative value consists in:
Designing the network to ensure the security of the databases of the National Taekwon-do Federation and to ensure the security of data transport within the communication network through practical implementation according to the materials presented in the chapters. The basic decisions and techniques used during the design period and the research methods that led to them were described.
This paper provides extensive analysis and recommendations to ensure good database security.

CUPRINS

INTRODUCERE

Cunoaștem bine faptul că activitățile diferitor organizații din lume (corporații, înreprinderi mari, mici, de stat), depind tot mai mult de tehnologiile informaționale, astfel putem deduce că problema protecției bazelor de date devine tot mai actuală. Pericolul de pierdere a informației confidențiale a devenit ceva obișnuit, însă și un lucru riscant pentru activitatea unei organizații. Fiecare esec în procesarea bazelor de date poate paraliza activitatea unor corporații întregi, bănci, servicii internet, ceea ce poate duce la pierderi financiare colosale. Deci, protecția datelor este o sarcină ce trebuie pus pe primul plan la crearea unei baze de date.

Astfel, pentru a găsi soluţii, iniţial e necesară stabilirea punctelor precare în bazele de date:

Limbajul SQL – un instrument puternic de interogare a datelor, însă de asemenea permite răufăcătorilor sa efectueze spargerea sistemului:

• Accesarea informaţiei cu ajutorul deducţiilor logice, potrivirea sau spargerea parolelor utilizatorilor bazei de date, a atacurilor îndreptate spre mărirea prilegiilor în sistem;

• Agregarea datelor, atacurile de tip SQL injection;

• Modificarea/înlocuirea datelor etc.

Gestiunea/controlul accesului la SGBD/BD/Server:

• Erori şi scăpări din vedere ale personalului de deservire şi a utilizatorilor;

• Acţiunile lucrătorilor necinstiţi, ofensaţi; acţiunile persoanelor străine;

• Furtul fizic, distrugerea informaţiei etc.

Atacurile asupra informaţiei care circula în reţea:

• Utilizarea conexiunilor existente la baza de date prin reţea, stabilite de utilizatorii autentificaţi;

• Interceptarea informaţiei în timpul parcurgerii ei prin reţea. Alte tipuri de atacuri: asupra sistemului de operare; blocarea accesului către date, supraîncărcarea buferului; hackerii şi virusurii. Securitatea bazelor de date poate fi asigurată prin

intermediul aplicării unor modele care 1 mai mult sau mai puţin corespund domeniului activităţii, politicii de securitate, importanţei informaţiei organizaţiei.

Actualitatea temei este determinată de faptul că în prezent asigurarea securității bazelor de date este necesară pentru protejarea informației entităților economice.

Un model simplu ar fi compus din 2 elemente: controlul accesului – unde fiecărui utilizator sau proces informaţional al sistemului i se atribuie un set de acţiuni permise, pe care le poate efectua în raport cu anumite obiecte; controlul autenticităţii – realizează dacă utilizatorul sau procesul care încearcă să efectueze o acţiune sau alta este anume acela pe care îl reprezintă. Un alt model mai sofisticat este acel de multinivel al securităţii bazei de date, care reprezintă un instrument foarte puternic, însă aduce unele incomodităţi în uşurinţa utilizării, productivitate, costuri etc. În aşa tipuri de sisteme informaţia este clasificată în diverse clase de importanţă şi, de obicei, se utilizează modelul lui Bell-LaPadula, care gestionează subiecţii, procesele, obiectele. Aplicarea modelelor se poate efectua fie direct în SGBD-ul / baza de date respectivă, fie în sisteme informatice aparte, proiectate şi exploatate în special pentru a asigura protejarea informaţiei. Metodologii de combatere a riscurilor şi atacurilor asupra bazei de date le putem clasifica în linii mari în 3 categorii:

1. Securitatea bazei de date şi a SGBD – scanarea DB, auditul vulnerabilităţilor, monitorizarea activităţilor, controlul accesului.

2. Auditul vulnerabilităţilor reţelei şi a sistemului de operare – mecanisme bazate pe scanarea reţelei şi exteriorul DB-ului. Rezultatele sunt examinări, rapoarte, determinarea punctelor slabe.

3. Criptarea bazei de date – care include un sistem de management al cheilor ce suporta o varietate de algoritmuri de criptare. De asemenea, am putea împărţi metodele şi după modul de aplicare: Tehnice:

1. Amplasarea serverelor de BD în segmente de reţea protejate şi securizarea lor.

2. Back-up. Aplicarea tehnologiilor de Cluster Systems. Tirajarea datelor.

3. Utilizarea metodelor eficiente de autentificare (server/OS authentification, parole cu un numar suficient de simboluri, certificate, chei criptate, dispozitive-chei etc.). Administrative:

1. Standartizarea cu ISO 17799, ISO 27001 (certificarea oficială a sistemelor de securitate informaţională).

2. Urmărirea transmiterii informaţiei prin canale de comunicaţie. Înregistrarea evenimentelor desfăşurate în cadrul SI. Auditul cererilor către SGBD.

Înregistrarea activităţilor utilizatorilor – permite de a omite în unele cazuri potenţialele cazuri de 2 atac asupra bazei de date sau de a investiga încălcările comise deja.

3. Determinarea cazurilor când informaţia nu este utilizată corect.

4. Delimitarea mediilor de administrare şi de dezvoltare.

5. Excluderea cazurilor de integrare a diverselor servicii corporative pe serverul unde e instalat 6. SGBD-ul.

7. Organizarea unei politici eficiente de acordare a drepturilor/rolurilor pentru diverse grupuri de utilizatori. După standartele intenţionale, se disting 3 categorii de roluri: proprietarul informaţiei; răspunzătorul de securitatea informaţiei; cel care utilizează informaţia. Software: 1. Configurarea mecanismelor proprii de protecţie a bazelor de date (drepturile de acces, privelegiile). Avantaje: precizie, acoperire totală (a scopurilor). Dezavantaje: viteză, complexitate (dimensiuni). 2. În etapa de proiectare să se ia în consideraţie de către proiectanţi/programatori evitarea afişării mesajelor de eroare clienţilor într-un mod care ar putea să divulge unele detalii despre sistem, scheme etc.; 3. Cifrarea bazei de date. Avantaje – un sistem sporit de securitate; dezavantaje: în caz că se defectează serverul sau cade sistemul, e greu de restabilit dacă are nevoie de o aplicaţie în plus care va gestiona cheile, viteza, indexarea. 4. Analiza protecţiei bazelor de date cu ajutorul unor instrumente, aplicaţii, sisteme de audit şi control de acces care pot permite: analiza evenimentelor critice, modelarea acţiunilor răufăcătorilor externi, analiza optimizărilor efectuate în SGBD şi OS, identificarea utilizatorilor necunoscuţi, scanarea centralizată, viziunea

asupra securităţii reţelei dintr-o parte etc. şi care pot răspunde la întrebări de tipul: ce baze de date sunt în reţea?; cât de corect e configurat SGBD-ul?, e posibil atacul SGBD-ului dv prin reţea?, corespunde configurarea SGBD-ului dv. cu politica de securitate?, e posibil ca utilizatorii „să înconjoare" mecanismele de protecţie a SGBD-ului şi SO?, care e rezultatul ataşării la SGBD a diverselor mecanisme de protecţie? etc.

Prin urmare, pentru a asigura securitatea bazei de date, trebuie întreprinși anumiți pași care vor ajuta la evitarea încălcării bazei de date: stabilirea accesului la elementele bazei de date, introducerea unei parole specifice, criptarea datelor și a programului.

Scopul lucrării este de a obține o rețea de comunicare privată în cadrul unei instituții utilizând rețeaua privată între agențiile publice asigurând siguranța transportului de date.

Lucrarea de faţă se axează pe următoarele **obiective**:

- Implementării unei rețele private în cadrul unei instituții
- Asigurarea siguranței transportului de date
- Implementarea soluțiilor de modernizare a rețelei de comunicații virtuale
- Examinarea tehnologiilor şi diverselor metode pentru a asigura o bună protecție a bazelor de date.

În cercetarea și redactarea subiectului propus, am folosit o varietate de metode de cercetare care permit o abordare complexă și un studiu detaliat al subiectului lucrării. Astfel voi menţiona următoarele metode: metoda inductivă-deductivă în baza analizei şi sintezei informaţiilor ştiinţifice şi doctrinare; metoda descriptivă; metoda observaţiei şi analizei.

CONCLUZII

Asigurarea securității bazelor de date ale Federației Naționale de Taekwon-Do este o responsabilitate importantă pentru a proteja informațiile sensibile și a asigura o funcționare eficientă a organizației. Prin luarea unor măsuri adecvate de securitate și prin colaborarea cu experți în domeniu, se poate asigura o protecție adecvată a bazelor de date ale Federației Naționale de Taekwon-Do.

Federația Națională de Taekwon-do are sediul central în or.Chișinău, iar celelalte filiale se află în localități la distanțe mari și implimentarea acestu proiect permite circulația informațiilor între filiale cu o viteză foarte înaltă. Tehnologia VPN funcționează pe baza protocoalelor standard sau printr-o rețea privată a furnizorului de servicii de internet (ISP) pusă la dispoziția publicului.

Unul din marele avantaje a acestui sistem este faptul că el permite conectarea utilizatorilor

6 mobili, a utilizatorilor îndepărtaţi, a diferitor parteneri, astfel încât ușurează activitatea acestora.

Este important ca bazele de date ale Federației Naționale de Taekwon-Do să fie protejate împotriva accesului neautorizat, a modificărilor ilegale sau a pierderii de informații. Pentru a asigura securitatea acestor baze de date, s-au luat în considerare următoarele măsuri:

-Implementarea unui sistem de autentificare și autorizare puternic, care să permită accesul doar utilizatorilor autorizați la anumite informații sau funcționalități.

-Utilizarea criptării pentru a proteja informațiile sensibile, precum parolele de acces sau datele personale ale utilizatorilor.

-Utilizarea măsurilor de protecție împotriva atacurilor cibernetice, cum ar fi firewall-urile și sistemele de detectare a amenințărilor.

-Implementarea unui sistem de backup și recovery pentru a asigura posibilitatea de a recupera informațiile în cazul unei pierderi sau a unei defecțiuni a sistemului.

-Instruirea personalului în privința practicilor de securitate cibernetică adecvate și promovarea unei culturi de securitate în cadrul organizației.

Echipamentul CISCO utilizat în acest proiect este scalabil și permite extinderea rețelei în orice moment. Cu ajutorul unui sistem VPN wireless, toate informațiile vor ajunge întotdeauna la timp și fiecare angajat va fi pe deplin informat.

Sistemul dezvoltat este foarte flexibil și are adaptabilitate avansată la mediul de implementare. Sistemul funcționează cu aproape orice tip de rețea existent. Este conceput pentru întreținerea tehnologiilor în curs de dezvoltare cu capacitatea de a analiza traficul în orice moment.

Prin luarea acestor măsuri concrete, Federația Națională de Taekwon-Do poate asigura protecția adecvată a bazelor sale de date și poate încredința utilizatorilor săi că informațiile lor sunt în siguranță.

BIBLIOGRAFIE

Surse bibliografice:

1. Thom Thomas - „Primii paşi în securitatea reţelelor”, Editura Corint, Bucureşti, 2005.
2. Tatiana Rădulescu - “QoS în reţelele IP multimedia” -, H.G. Coandă, Editura Albastră, Cluj- Napoca , 2007.
3. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
4. Andrew Tanenbaum - „Reţele de calculatoare” -, Ediţia a IV-a, Byblos, 2003
5. Virgil Dobrotă - „Reţele digitale în telecomuncaţii” -, vol.III OSI şi TCP/IP, Editura Mediamira, Cluj-Napova, 2002.
6. Năstase F.,- „Arhitectura reţelelor de calculatoare”, Bucureşti: Editura Economică, 1999.
7. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
8. Ionescu, Dan –”Retele de calculatoare”, Alba Iulia: Editura All 2007.
9. Georgescu, Ioana.-” Sisteme de operare”, Craiova: Editura Arves, 2006.

Surse electronice:

1. http://customs.md/despre/adrese.php?lang=ro
2. www.cisco.com/warp/public/471/ vpn-3k2-ios-nem-lea.html
3. www.pcnet.ro

4. www.agora.ro
5. www.hypervivid.com/ policy/VPN-policy/
6. vpn.web.cern.ch/vpn/status/
7. www.sparq.com.tw/products/ voice_vpn.html
8. www.allmedia.cc/vpn.html
9. www.comsol.nl/services/ security/vpn.htm
10. www.smoothwall.org/ about/screenshots
11. http://www.citforum.ru/security/cryptography/yaschenko/1.html
12. www.netmarks.co.jp/prdct_srvc/ prdct_info/product/img/vpn.gi
13. www.homenethelp.com/web/review/ images/routefinder-vpn.gif
14. www.gits.net.th/services/ intranet_service.html
15. www.cisco.com/.../warp/public/ 3/jp/solution/ent/tech/vpn/
16. http://www.interhack.net/pubs/fwfaq/
17. www.checkpoint.co.jp/products/ b_img/vpn-1_clients_lg.gif
18. www.sitaranetworks.com/ solutions/vpn.cfm
19. www.ibm.com/servers/aix/products/ ibmsw/security/vpn/
20. www.cytanet.com.cy/ services/vpn.html
21. www.atlas.et.ee/lahendused/ atlas_vpn.html
22. www.centerweb.it/vpn.shtml
23https://www.rasfoiesc.com/educatie/informatica/baze-de-date/Securizarea-bazelor de date
24.https://taekwondo-moldova.org