Universitatea Tehnică a Moldovei

Sistem de autentificare bifactorială de securizare a sistemelor informaționale

Student:

A. NIRCA

Conducător:

E. GUȚULEAC

Chişinău - 2020

ADNOTARE

La teza de masterat: „Sistem de autentificare bifactorială de securizare a sistemelor informaționale” elaborat Nirca Anton, Chișinău, 2020.

Cuvinte cheie: securitate cibernetică, atac cibernetic, aplicație, sistem informațional, sistem de operare, autentificare multifactorială, terorism cibernetic, sistem computerizat.

Lucrarea de față are drept scop proiectarea și implementarea unui sistem de autentificare pe mai multe etape. Din cauza că uneori astfel de sisteme sunt destul de greu de implementat, iar la partea financiară se evedențiază un cost destul de mare pentru ele, multe compani care nu dispun de un buget mare de finanțe nu își pot permite astfel de sisteme. Drept scop al proiectului este sporirea nivelului de securizare în cadrul procesului de logare a utilizatorilor.

Tehnologiile utilizate: Limbajul de programare PHP, instrumentele Composer, Laravel, XAMPP pentru dezvoltarea sistemului și creearea bazei de date necesare, precum și generarea QR-code pentru un nivel mai sporit de securitate.

Memoriul explicativ conţine adnotarea, declarația de onestitate, lista de figuri, lista de abrevieri, introducere, 3 capitole, concluzii, bibliografie cu 30 titluri, dintre care 70 pagini text de bază, 46 figuri şi 3 anexă.

Capitolul 1 definește cadrul elaborării lucrării, baza de cunoștințe necesară pentru a elabora sistemul, cu descrierea generală a utilităților ce urmează a fi implementate, totodată este descrisă argumentarea temei prin exemple reale de atacuri cibernetice produse în România care au stat la baza creării proiectul.

Capitolul 2 definește analiza integrală a diverse tipuri de atacuri cibernetice, metode de protecție și aplicații necesare pentru a preveni astfel de vulnerabilități în sistemele companiilor mari și mici.

Capitolul 3 descrie structura generală a sistemului, inclusiv toate metodele de formare, planificare, creare a aplicațiilor, totdodată sunt descrise instrumentele necesare pentru proiect, paginile oficiale de unde pot fi descărcate și ghidul de utilizare a sistemului.

ANNOTATION

At the master project: "Bifactorial authentication system for securing information system" elaborated by Nirca Anton, Chișinău, 2020.

Keywords: cyber security, cyber attack, application, information system, operating system, multifactor authentication.

This paper aims to design and implement a multi-stage authentication system. Because sometimes such systems are quite difficult to implement, and the financial part shows a fairly high cost for them, many companies that do not have a large budget of finance can not afford such systems. The aim of the project is to increase the level of security in the user login process.

The technologies used are: PHP programming language, Composer, Laravel, XAMPP tools for system development and creating the necessary database, as well as generating QR-codes for a higher level of security.

The explanatory memorandum contains the annotation, the statement of honesty, the list of figures, the list of abbreviations, the introduction, 3 chapters, conclusions, bibliography with 30 titles, of which 70 pages of basic text, 46 figures and 3 annex.

Chapter 1 defines the framework of the elaboration of the paper, the knowledge base necessary to elaborate the system, with the general description of the utilities to be implemented, at the same time it describes the argumentation of the theme by real examples of cyber attacks produced in Romania.

Chapter 2 defines the comprehensive analysis of various types of cyber attacks, protection methods and applications needed to prevent such vulnerabilities in the systems of large and small companies.

Chapter 3 describes the general structure of the system, including all methods of training, planning, creating applications, also describes the tools needed for the project, the official pages where they can be downloaded and the user guide of the system.

Cuprins

INTRODUCERE

La etapa actuală a evoluție omenirei, securitatea informațională a devenit un factor cu o deosebită importanță pentru orice utilizator, înterprindere, mica afacere, buissnes sau stat. Informația simplă cât și cea clasificată precum și datele cu caracter personal sunt pastrate în diferite locuri special amenajate cum sunt arhivele și datacentrele. O problemă cu impact major a tuturor, constă în pierderea și furtul informației (de la conversațiilor personale până la date cu caracter personal). Informațiile pot fi divulgate sau folosite pentru șantaj atât direct de infractor/răufăcător cât și publicate în spațiul online. Furturile online și crimile cibernetice au provocat prejudicii de miliarde de dolari doar în anul 2017 (atacurile NotPetya și BadRabbit), astfel, toate firmele de securitate cibernetică au devenit o potențială ținta a hackerilor, la fel se evedințiază o sursă a atacurilor virtuale care sunt țările autoritare. Anual se înregistrează până la 6 milioane de tentative de atac cibernetic doar în Republica Moldova, malware-ul pentru furtul de informații, phishingul, exploituri zero-day, cripto-jacking-ul etc [2].

Pentru a putea asigura securitatea informației, a devenit necesar de a implementa diferite măsuri de protecție a ei. În așa caz, ne referim la un sistem de control al accesului a spațiilor sau mediilor unde este păstrată informația, însă nu uităm că progresul tehnic este în creștere dinamică așa că este necesar periodic de îmbunătățit aceste sisteme. O astfel de îmbunătățire a devenit și sistemul de autentificare multifactorială.

Obiectivul principal al acestei lucrări constă în crearea și implementarea unui sistem de autentificare bifactorială, care urmează sa fie simplu în utilizare și disponibil pentru orice tip de utilizator și în orice domeniu dorit. Sistemul are posibilitatea de a fi adaptat la controlul accesului în rețele de socializare, conturi ale companii, accesului în blocul de trai sau spații de păstrare a serverelor.

Conţinutul disertației de master include toate compartimentele necesare, structurate logic şi coerent, se descrie metodologia cercetării care a fost bazată pe literatura de specialitate prin abordarea informației din diferite puncte de vedere. În primul capitol se descriu aspectele generale a resurselor informaționale și a securizării acestor rețele, se menționează unele tehnici de securitate și este dusă tangenta dintre societate modernă și influența atacurilor asupra ei. La fel este descris prin exemple concrete de atacuri cibernetice asupra mai multor state impactul și prejudiciu care a fost provocat, din cauza că nu au respectat unele măsuri de precauție și nu au folosit apdaturile la timp oportun.

În capitolul doi este descrisă o sinteză a atacurilor informatice și a modalităților de înlăturare sau prevenire ale lor, s-a efectuat analiza și descrierea de nivel înalt tehnicilor de securizare a rețelelor informaționale. Sunt menționate elementele de inovație și cercetare științifică ce reprezintă utilizarea instrumentelor de securizare a rețelelor informatice. În urma cercetărilor

efectuate am luat cunoștință cu diverse tipurile de atacuri informaționale cum ar fi Dos, DDos, MITM, SYN FLOOD și respectiv metode de prevenire, depistare și contracarare a acestor atacuri. Modul fiecăruia de funcționare și estimarea prejudiciului ce poate fi pricinuit din partea lor.

În capitolul trei au fost evedențiate unele aspecte importante în selectarea și implementarea mecanismelor de securitate, de ce este din punct de vedere financiar mai oportun de folosit sistem de autentificare multifactorială. Este descrisă metoda de elaborare a unui sistem cu autentificare multifactorială, procedeele și programele care au fost folosite la elaborarea lui, și un ghid care descrie detaliat cum funcționează sistemul prin exemple concrete și imagini pentru o înțelegere mai eficientă.

Scopul efectuării lucrări de disertație rămâne a fi prevenirea și contracararea accesului neautorizat în orice sistem informatic. Autentificarea multifactorială este descrisă printr-o modalitate puternică de securizare a sistemului în acest sens. În orice întreprindere sau companie obiectivul principal constă în asigurarea securității informației, a datelor cu caracter personal, a colaboratorilor și a resurselor, așa că securitatea informației este un element de prim plan.

BIBLIOGRAFIE

1. https://www.iso.org/members.html.
2. Colun Tatiana. 6 th International Conference "Telecommunications, Electronics and Informatics" ICTEI 2018 "Securitatea sistemelor informatice - pilon de bază al siguranței informaționale" pag. 357.
3. https://lerablog.org/technology/data-security/how-to-protect-your-business-against-ddos-attacks/.
4. Jim WEBBER, Savas PARASTATIDIS, Ian ROBINSON VPN in Practice - Hypermedia and Systems Architecture, Third Edition NY – December 2014, pag. 23-25.
5. Richard Bejtlich The Practice of Network Security Monitoring: Understanding Incident Detection and Response, 2013, pag. 310.
6. Parlamentul European, Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, studiu pentru Comisia LIBE, septembrie 2015.
7. http://www.techiesjournal.com/social-engineering-attacks/.
8. https://networkguru.ru/dos-ataka-tcp-syn-flood/.
9. https://vasexperts.ru/blog/kak-vzlomat-vashu-perepisku-mitm-ataka/.
10. https://cryptographybuzz.com/attacks-dns-rebinding/.
11. https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-arp-spoofing/.
12. https://www.rcast.net/anti-ddos-protection.
13. https://www.kaspersky.ru/enterprise-security/ddos-protection.
14. https://www.cloudflare.com/ru-ru/ddos/.
15. https://community.fs.com/ru/blog/what-is-vpn-router-and-why-you-need-it.html.
16. https://blog.themarfa.name/kak-rabotaiet-vpn-i-pochiemu-eto-luchshie-tor-ili-proxy/.
17. https://pickmycablemodem.com/home-firewalls/.
18. https://www.nexor.com/firestorm-next-generation-firewall-vulnerability/.
19. https://alemba.help/help/content/topics/installation%20and%20upgrade/install%20and%20upgrade/install%20appendixb-%20config%20dmz.htm.
20. http://azuredummies.com/2016/01/29/introduction-to-azure-multifactor-authentication-concept/comment-page-1/.
21. https://laravel.com/.
22. https://getcomposer.org/.
23. https://www.apachefriends.org/ru/index.html.
24. https://ionutsblog.wordpress.com/2011/12/01/implementare-protocol-radius-pe-infrastructura-wireless/.

25. https://www.tutsmake.com/ laravel-php-simple-qr-codes-generate/.
26. https://vegibit.com/how-to-create-user-registration-in-laravel/.
27. Dmitry Garbar, Beneficii Laravel, https://belitsoft.com/laravel-development-services/10-benefits-using-laravel-php-framework.
28. Jeremiah Doriam The Social Engineer's Playbook: A Practical Guide to Pretexting, 2014, pag. 32.
29. Алексей Петровский Эффективный хакинг для начанающих и не только, Kiev 2014, pag. 322.
30. Gil HELD, Kent HUNDLEY Arhitecturi de securitate, Editura Teora, 2003, pag. 33.