Universitatea Tehnică a Moldovei

SOLUȚIE DE PROCESARE ȘI ANALIZĂ A FIȘIERELOR JURNAL

SOLUTION FOR JOURNAL FILE PROCESSING AND ANALYSIS

Masterand:

Țurcanu Constantin

Conducător:

lector universitar Putere Alexandru

Chişinău 2020

Ministerul Educaţiei, Culturii şi Cercetării
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
dr.conf.univ. Ion Fiodorov.
„20" decembrie 2019

SOLUȚIE DE PROCESARE ȘI ANALIZĂ A FIȘIERELOR JURNAL

Teză de master în Securitate Informațională

Masterand: (Țurcanu Constantin)

Conducător (Putere Alexandru)

Chișinău 2020

Rezumat

Această lucrare descrie proiectarea și realizarea unei aplicații desktop de gestionare a fișierelor jurnal. Fișierele jurnal (log) sunt o resursă importantă pentru managementul sistemelor informatice, oferind informații atât despre simple evenimente, cât și despre cele care au intenții rele.

Astfel, memoriul explicativ este structurat în trei capitole.

Capitolul 1 conține o analiză a utilitei Windows Log Viewer, a tipurilor de fișiere jurnal și sunt identificate neajunsurile în cazul gestionării fișierelor log din Windows. Neajunsurile scoase în evidență au servit la descrierea cerințelor funcționale ale aplicației, prin propunerea unor instrumente de sortare și filtrare după mai multe criterii, astfel încât un administrator sau un ofițer de securitate să poată genera mai eficient rapoarte privind activitățile înregistrate de log-uri pe paltforma Windows.

Capitolul 2 descrie proiectarea aplicației. Diagramele prezentate în acest capitol prezintă descrierea comportamentală și structurală a sistemului informațional. Aici sunt prezentate activitățile și stările de tranziție ale aplicației, dar și fluxurile de mesaje între componentele sistemului informațional.

Capitolul 3 prezintă în mod detaliat realizarea și utilizarea aplicației. Sistemul este elaborat pe baza tehnologiilor informaționale moderne, precum C#, *SQLite*. În mod succint este descrisă arhitectura sistemului informațional, componentele sale precum și detalii de implementare la nivel de cod sursă. Este prezentată interfața sistemului și modul în care interacționează componentele sistemului.

Sistemul elaborat în cadrul tezei de master este destinat pentru efectuarea procesării și analizei log-urilor Windows. Poate fi utilizat ca instrument de sortare a lor în funcție de diferite criterii, îmbunătățirea eficienței unui sistem sau pentru determinarea aplicațiilor care cel mai des înscriu erori în jurnal, pentru prevenirea riscurilor și ca instrument de investigare în cazul infracțiunilor informatice.

Abstract

This paper describes the design and development of a desktop application for managing the log files. The log files are an important resource for information systems management, providing information about both, simple and those with bad intent events.

So, the explanatory memo is structured in three chapters.

Chapter 1 contains an analysis of the Windows Log Viewer utility, the log file types and identifies all the shortcomings for log file management in Windows.

The shortcomings highlighted were used to describe the functional requirements of the application by proposing tools for sorting and filtering according to different criteria, such as an administrator or a security officer can more efficiently generate reports on activities recorded logs on Windows platform.

Chapter 2 describes the design of application. The diagrams presented in this chapter present the behavioral and structural description of the information system. Here are presented the activities and transition states of the application, as well as the message flows between the components of the information system.

Chapter 3 describes in detail the implementation of the application. The system is developed based on modern information technologies such as Microsoft C#, SQLite. The information system architecture, its components as well as implementation details at source code level are briefly described. The system interface and how the system components interact are presented.

The system developed under the license thesis is intended for processing and analyzing Windows logs. It can be used as a tool for sorting them according to different criteria, improving the efficiency of a system, or for determining applications that most often include log errors, risk prevention, and as a tool for investigating cybercrime.

CUPRINS

INTRODUCERE

Securitatea informației se ocupă cu protejarea mediului informatic împotriva accesului neautorizat, dezvăluirea, întreruperea, modificarea sau distrugerea datelor și a sistemelor. Nevoia de analiză, monitorizare, prevenire și protecție a mediului digital este foarte necesară și urgentă. Din acest motiv trebuie să avem la dispoziție instrumentele necesare pentru a putea fi pregătiți într-o perspectivă de timp adecvat.

Pentru a putea realiza un program de securitate eficient este nevoie de politici, proceduri, practici, standarde, descrieri ale sarcinilor şi responsabilităţilor de serviciu, precum și de o arhitectură generală a securităţii.

În orice sistem informatic, pentru asigurarea securității și prevenirea riscurilor este necesar să fie activat și configurat un sistem de scriere a log-urilor, cum ar fi de exemplu, Windows Event Logs în SO Windows.

Un fișier log este de fapt un document creat în mod automat de un sistem care dispune de asemenea opțiuni și care pe toată perioada funcționării sistemului acumulează date precum: ip-uri care se conectează la server, browser-ele folosite, datele care s-au cerut/trimis către server, cantitatea de date servită/solicitată, ora, minutele, secundele în care s-a transmis fiecare byte, erorile apărute, solicitările unor aplicații de resurse adăugătoare, sursa fiecărui vizitator etc., toate acestea într-un simplu fișier, care poate fi deschis cu notepad și care uneori ajunge la dimensiuni de ordinul Giga! Fișierele de tip jurnal nu pot fi accesate de către utilizatori deoarece oricine s-ar putea folosi în mod “unfair play” de ele. De aceea datele vizitatorilor trebuiesc protejate.

Chiar dacă datele sunt foarte multe, filtrate și analizate de un profesionist, acestea relevă foarte multe informații atât despre simple evenimente, cât și despre cele cu intenții infracționale. Examinarea atentă a log-urilor relevă situația din sistemul informatic, iar drept dovadă, există departamente care se ocupa doar de acest lucru – de analiza log-urilor. Scopul ar fi de a îmbunatați eficiența unui sistem sau determinarea aplicațiilor care cel mai des înscriu erori în jurnal.

Pe de altă parte, atacurile și pierderile de informații cresc constant. Lupta cu criminalitatea informatică este o problemă actuală și acută. Tot mai multe tehnologii şi instrumente software avansate sunt disponibile în spațiul Internet și puse la îndemâna oricui. Orice persoană, cu puţină experienţă în domeniul informatic, utilizând astfel de unelte poate ataca și provoca daune unui sistem neprotejat.

Deși principiile stabilite de actele normative în vigoare pentru efectuarea unei verificări sau percheziții nu se schimbă în mediul electronic, trebuie totuși utilizate procese mentale și aptitudini noi. Astfel, daca în cazul unei percheziții clasice, anchetatorul poate vizualiza obiectele ce ar putea constitui probe, în situația unei percheziții efectuate într-un mediu informatic, dispozitivele de stocare a probelor electronice s-ar pute să nu fie atât de evidente pentru anchetator, mijloace importante de probă putând fi omise sau deteriorate în procesul de percheziție.

Culegerea datelor în mediul informatic și transformarea acestora în probe se va face în funcție de indiciile existente în cazul investigat, caracteristicile acestora determinând procedura ce trebuie urmată.

În cazul analizei fișierelor jurnal (log) trebuie avute în vedere câteva reguli de baza:

- Se va lucra numai cu copii ale fișierelor analizate, iar datele originale se vor stoca în locuri sigure. De asemenea, este recomandabil ca datele obținute să fie organizate și stocate sub forma unor baze de date sau tabele, care să permită sortarea lor în funcție de diferite criterii. Utilizarea unui software de analiză a datelor culese, în vederea identificării legăturilor existente între aceste informații, se poate deveni de mare valoare pentru investigator.
- Evenimentele investigate vor fi regrupate pentru a stabili daca acestea se încadrează într-o linie cronologică firească;
- Se va stabili ordinea cronologică a evenimentelor investigate pentru fiecare element în parte și ulterior pentru toate fișierele de log, recalculând toate informațiile în funcție de tipul zonal în care se lucrează, cu sincronizările și corecțiile necesare;
- În cele din urmă se va verifica dacă ordinea cronologică a informațiilor este respectată de toate fișierele jurnal, în succesiunea firească a acestora.

De altfel, multe companii sunt obligate să păstreze logurile o perioada de timp îndelungată, deoarece acestea pot fi folosite ca probă. De exemplul Youtube vs Viacom – compania care a dat în judecată platforma de video sharing pe motiv că ar promova materiale piratate. În acest caz, pentru a-și demonstra nevinovăția, Youtube a adus la tribunal loguri care în total ajung la cantități de ordinul terra bytes.

Nu e o problemă de scrierea evenimentelor într-un jurnal, ci e foarte important de a putea face analiza și filtrarea masivului mare de date. Această problemă o poate soluționa un analizator de loguri.

Obiectivul proiectul de master este de a evidenția importanța unui Analizator al Log-urilor sistemului de operare Windows. Sistemul vine să ofere instrumente de sortare a evenimentelor după mai multe criterii, care, la rîndul lor, pot fi filtrate după anul și luna cînd au fost generate. De asemenea, oferă posibilitatea de grupare după tipul log-urilor: informaționale, de eroare etc. și de utilizare a filtrelor „friendly-user” cu posibilitatea de a fi reprezentate în formă grafică.

CONCLUZII

Din moment ce trăim și facem parte din societatea noilor tehnologii informaţionale, nu ne miră deloc faptul că multitudinea de programe care sunt realizate zi de zi facilitează procesul de lucru din cadrul fiecărei instituţii. Pentru implimentarea unui nou produs program, e nevoie să se ţină cont de politica acestuia şi de stilul lui de activitate. Sistemul de evidenţă din cadrul instituţiei, prevede delimitarea evidentă a gradului de responsabilitate şi nivelului de competenţă necesară pentru exercitarea fiecărei funcţii.

În rezultatul efectuării acestei teze de master, a fost proiectată o aplicație de gestionare a fișierelor jurnal, a log-urilor. Ca scop s-a pus în prim plan sarcina de a fi elaborat un concept al analizei, pentru ca mai târziu acesta să fie dezvoltat și să ajungă la ultima etapă de punerea în exploatare. Modelarea și analiza a permis efectuarea cerinţelor faţă de produs, crearea scenariilor de lucru și reprezentarea acestora.

În concluzie putem marca faptul că cel mai important pas este legat de realizarea sistemului ce permite utilizatorilor de a conlucra eficient, de a comunica și sigur de a aduce folos celor ce au nevoie de unele resurse informaționale și celor ce oferă posibilitatea de a înțelege conceptul de log. Proiectarea unui astfel de sistem a permis să înţelegem mai bine necesităţile impuse, ordinea de executare a operaţiunilor.

Fișierele jurnal sunt unelte foarte valoroase pentru a monitoriza performanţele și securitatea sistemelor care adesea sunt inferior utilizate datorită complexităţii și volumului mare de date și evenimente care au loc.

Managementul jurnalelor de evenimente presupune satisfacerea câtorva obiective:

- securitatea sistemului informațional;
- monitorizarea stării sistemului;
- conformitatea cu legislația în vigoare;
- posibilitatea investigării judiciare.

Astfel, un volum mare de fișiere log reprezintă o sursă foarte valoroasă de informaţie pentru administratorii de sistem. Un management eficient al infrastructurii ajută să se menţină sisteme securizate şi disponibilitate maximă, permiţând totodată organizaţiilor să îşi indeplinească obligaţiile de legalitate. Din aceste considerente, sunt foarte necesare

instrumentele care ar asigura un management cât mai eficient al log-urilor – un analizator de fișiere jurnal.

Sistemul de procesare și analiză a log-urilor realizat în cadrul proiectului de master constă din două module, unul de procesare și calcul analitic, altul de analiză. Analizatorul log-urilor oferă posibilitatea să sorteze log-urile după diferite criterii, să le filtreze după anumite perioade și să reprezinte rezultatele prin grafice analitice care vin să acorde un ajutor substanțial administratorilor de sistem și specialiștilor din securitate.

Beneficiile care sunt aduse de sistemul realizat, sunt destul de importante și asigură:

- stocarea centralizată a log-urilor printr-o structură bine definită;
- procesare incorporată ce permite estimarea numărului de log-uri după tipuri, perioade etc.
- sortarea log-urilor în funcție de diferite criterii;
- creșterea disponibilității infrastructurii informatice și identificarea problemelor;
- posibilitatea de analizare și detectare eficientă a incidentelor de securitate;
- analiza în detaliu pentru a identifica cine este responsabil de apariția anumitor incidente;
- monitorizare şi management rapid şi eficient al sistemelor;
- colectarea datelor necesare în cazul investigațiilor infarcțiunilor informatice.

Drept rezutat al aceste teze, sistemului de managemet al logurilor, procesarea și utilizarea rezultatelor, atât la nivel de prevenție precum și la nivel de produs finit ca material probator, este necesar de a fi aplicat și utilizat pentru sistemele de operare, diverse aplicații, sisteme informaționale, în cadrul Instituțiilor Publice, Organelor de aplicare a Legii, în deosebi Centrului de Combatere a crimelor Informatice din subordinea Inspectoratului Național de Investigații, Serviciul tehnologii Informaționale al MAI, precum și a altor subdiviziuni de profil din cadrul Ministerului Afacerilor Interne.

BIBLIOGRAFIE

1. How to Use Event Viewer in Windows 10 [citat 2019-09-15]. Disponibil pe Internet: https://www.dummies.com/computers/operating-systems/windows-10/how-to-use-event-viewer-in-windows-10/
2. Codrut Neagu, Cum lucrezi cu Event Viewer (Vizualizatorul de evenimente) în Windows [citat 2019-09-15]. Disponibil pe Internet: https://www.digitalcitizen.ro/primii-pasi-lucrul-event-viewer-windows
3. Event Log File Format [citat 2019-10-09]. Disponibil pe Internet: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-log-file-format
4. Reading from the Event Log [citat 2019-10-09]. Disponibil pe Internet: https://docs.microsoft.com/en-us/windows/win32/eventlog/reading-from-the-event-log
5. ReadEventLogA function [citat 2019-10-09]. Disponibil pe Internet: https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-readeventloga
6. Exportați, ștergeți și măriți dimensiunea pentru jurnalele de evenimente din Windows [citat 2019-11-05]. Disponibil pe Internet: http://ro.tipsandtricks.tech/exportati-stergeti-si-mariti-dimensiunea-pentru-jurnalele-de-evenimente-din-windows
7. Despre limbajul C# şi platforma .NET [citat 2019-11-19]. Disponibil pe Internet: http://www.ls-infomat.ro/user/content/e9efcsharp.pdf