ASPECTE PRIVIND SECURITATEA ACCESULUI LA CONȚINUTUL EDUCAȚIONAL MEDUCA

Mihai Jitaru

Mihai.Jitaru@computerland.ro

MBL Computers, Bucureşti

Dragoş Ioniță

Dragos.Ionita@training.computerland.ro

MBL Computers, Bucureşti

Nicoleta Iacob

Nicoleta.Iacob@training.computerland.ro

MBL Computers, Bucureşti

George Manea

George.Manea@computerland.ro

MBL Computers, Bucureşti

Rezumat: Lucrarea prezintă o soluție de securizare a accesului la conținutul educațional, implementată pe portalul MEDUCA din cadrul Centrului pilot de difuzare de conținut digital. Soluțiile identificate au fost folosite în finalizarea implementării infrastructurii IT pentru găzduirea portalului, dar şi pentru accesul în special din Internet la serviciile oferite. Portalul MEDUCA a fost realizat în cadrul proiectului de cercetare MEDSCEN -"Cercetări aprofundate pentru crearea unui sistem educațional pilot în spațiul virtual pentru simularea scenariilor privind dezastrele naturale şi modului de acțiune a cetățenilor şi instituțiilor în situații de criză", în curs de realizare de către un consorțiu condus de Universitatea Națională de Apărare „Carol I" (UNAp) şi finanțat de ANCS prin CNMP.

Cuvinte cheie: eLearning, securitate, portal, model cadru.

Abstract: The paper presents a solution for providing secure access to the educational content, implemented on the MEDUCA portal of the Romanian Pilot Centre for Dissemination of Digital Content. The solutions identified have been used in completing the implementation of IT infrastructure needed to host the portal, and also to grant access, particularly through Internet, to the services of the portal. The MEDUCA portal was created under the MEDSCEN research project - "Thorough research for the creation of a pilot educational system within the virtual space in order to simulate scenarios concerning natural disasters and appropriate action planning procedures designed for citizens and institutions in crisis situations – a project that is under development by a consortium coordinated by the National Defence University of Romania "Carol I" and financed by ANCS (the National Authority for Scientific Research) through CNMP (the National Centre for Programme Management).

Keywords: eLearning, security, portal, framework

1. Introducere

Managementul securității sistemelor de eLearning, controlul accesului şi siguranța au atras tot mai mult atenția cercetătorilor şi dezvoltatorilor de aplicații Web, datorită noilor tendințe în dezvoltarea sistemelor educaționale şi necesității realizării de aplicații care să poată fi accesate şi utilizate la distanță [1]. Controlul accesului trebuie să prevină accesul neautorizat la resursele partajate [2]. Îndeplinirea unor asemenea cerințe într-un sistem de eLearning este o problemă deosebit de complexă, deoarece este necesar să se protejeze conținutul, serviciile şi datele personale nu numai pentru utilizatorii externi ai unui sistem, ci şi pentru utilizatorii interni inclusiv pentru administratorii sistemului [3,4,5].

Au fost identificate câteva strategii de abordare a problemei securității portalurilor:

a) abordare globală;
b) abordare punctuală;
c) abordare bazată pe niveluri funcționale sau arhitecturale.

Pentru a reduce riscurile de securitate în utilizarea şi administrarea sistemelor IT, cea mai bună strategie este cea de ansamblu (*security in depth*). Aceasta presupune evaluarea pe

ansamblu a infrastructurii IT (echipamente, rețea, software de bază), a aplicațiilor oferite şi clasificarea expunerii la riscuri de securitate. Pentru fiecare dintre riscurile identificate trebuie realizate planuri de măsuri, fie pentru reducerea expunerii la acele riscuri, fie pentru reducerea efectelor odată ce riscul s-a produs .

În cadrul proiectului de cercetare MEDSCEN -"Cercetări aprofundate pentru crearea unui sistem educațional pilot în spațiul virtual pentru simularea scenariilor privind dezastrele naturale şi a modului de acțiune a cetățenilor şi instituțiilor în situații de criză", în curs de realizare de către un consorțiu condus de Universitatea Națională de Apărare „Carol I" (UNAp) şi finanțat de ANCS prin CNMP, se urmăreşte dezvoltarea unui portal de cunoştințe care înglobează instrumente pentru crearea şi difuzarea de conținut digital standardizat din domeniul protecției şi reconstrucției în caz de dezastre care să ofere cetățenilor şi agenților economici acces la informații neclasificate asupra asistenței în caz de dezastre şi bune practici de răspuns la situații de dezastru care amenință individul şi societatea. Totodată, prin acest portal, vor fi create şi distribuite cursuri în format digital care vor viza cunoaşterea în domeniu, formarea culturii de protecție şi reconstrucție, noi metode de instruire şi evaluare pentru instituții implicate în managementul crizelor şi intervenția la dezastre, atitudine civică şi modelarea comportamentului uman în situații de criză, pe timpul acestora şi în perioada post-criză [6,7]. Pentru a proiecta şi implementa infrastructura IT, dar şi pentru abordarea globală a securității unui portal eLearning a fost identificat un model cadru în care sunt incluse toate componentele tehnologice şi procedurale necesare [8]. Capitolul al doilea al lucrării descrie configurările de securitate propuse şi implementate în sistemul MEDUCA în sistemul firewall, în sistemul de operare suport pentru portal, la nivelul unor servicii (de ex. DNS).

2. Aspecte privind securizarea sistemului MEDUCA

2.1 Introducere

În definirea şi implementarea măsurilor de securizare în cazul portalului MEDUCA am abordat o soluție globală. Am avut în vedere arhitectura sistemului MEDUCA dar şi nivelele funcționale ale acestuia. În acest sens am avut în vedere următoarele aspecte:

- organizarea sistemului ca un Data Center, echipamentele şi mediile de comunicație fiind încapsulate într-o structură compactă ce poate fi uşor izolată fizic.
- organizarea rețelei ce conține sistemele componente ale portalului sub forma unui Intranet, separat de Internet printr-un dispozitiv de tip firewall dedicat acestei funcțiuni.
- stocarea datelor se face pe un echipament de stocare plasat pe o rețea dedicată, separată de rețeaua Ethernet dedicată echipamentelor portalului.
- accesarea portalului de următoarele categorii de utilizatori:
  - utilizatorii care vor accesa resursele educaționale oferite în cadrul portalului pentru a le consulta (consultare),
  - utilizatorii parteneri în proiect care vor accesa portalul pentru a furniza materiale didactice noi spre a fi verificate şi apoi publicate pe portal (upload),
  - utilizatorii parteneri în proiect care vor verifica materialele didactice primite şi apoi le vor publica pe portal (administrare conținut portal),
  - utilizatorii parteneri în proiect care vor administra portalul (administrare utilizatori portal),
  - utilizatorii parteneri în proiect care vor administra infrastructura IT hardware şi software, dar şi configurările de securitate la nivelul infrastructurii IT (administrare infrastructură IT hardware şi software).

Securitatea sistemului MEDUCA este asigurată prin stabilirea politicilor de securitate pentru fiecare nivel arhitectural sau funcțional al sistemului. În general, aceasta poate fi descrisă ca un ansamblu de elemente, după cum urmează:

- sistemul de tip firewall;
- politicile de securitate la nivelul sistemelor de operare;

- securitatea portalului sau al serverelor şi aplicaţiilor web;
- măsurile de securitate avute în vedere în momentul programării şi particularităţile limbajului de programare ales;
- accesul fizic la infrastructura IT hardware;
- protecţia la şocurile şi fluctuaţiile alimentării cu energie electrică.

O altă abordare globală a securităţii se poate face folosind un cadru organizat pe niveluri (vezi figura 1). O astfel de abordare poate reduce şansa de succes a unui atacator, dar poate şi să crească riscul detectării unui atac.

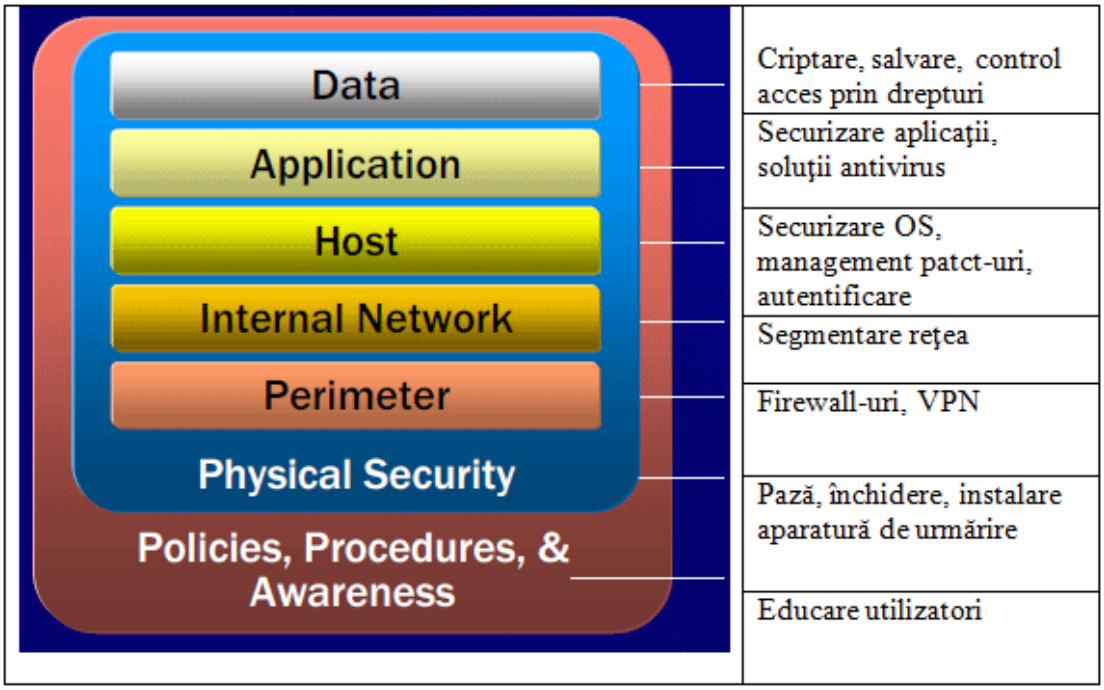

Figura 1. Cadru de organizare a securităţii folosind o abordare pe niveluri

2.2 Securizarea prin sistemul de tip firewall

Sistemul firewall MEDUCA este implementat pe un calculator separat ceea ce-i conferă o arie minimă de expunere la atacuri externe. Acesta analizează şi eventual transferă către server traficul de date provenit de la clienţi. În figura 2 este prezentat modul de conectare la Internet a portalului MEDUCA prin intermediul maşinii firewall.

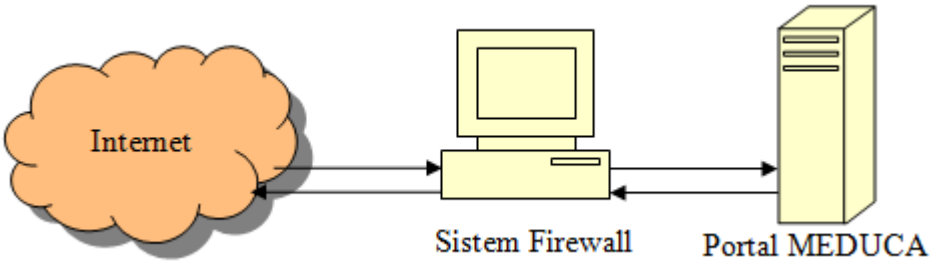

Figura 2. Conectarea portalului la Internet

În acest tip de arhitectură, oprirea sistemului firewall din orice cauză sau nefuncționarea acestuia conduce implicit la întreruperea fizică a transferului de date dintre rețeaua Internet şi portal.

Sistemul de operare de pe maşina firewall este Debian Linux 5.0 (April 11th, 2009), cu versiune de nucleu 2.6, un sistem de operare care are reputația de a fi sigur, compact şi stabil în timp. Pentru a elimina din riscurile de securitate care pot apărea în urma erorilor de programare la unele aplicații, s-au instalat numai acele pachete de aplicații care erau necesare pentru funcționarea optimă a firewall-ului.

O maşină de tip firewall nu trebuie să poată fi accesată din Internet, de aceea toate aplicațiile TCP/IP (toate porturile de aplicații) au fost închise. Astfel a fost eliminată posibilitatea de a se încerca atacarea maşinii din rețea în vederea câştigării accesului pe aceasta. O schema mai detaliată cu tipurile de accese permise prin configurarea actuală a sistemului firewall MEDUCA este prezentată în figura 3.

De fapt, un firewall, lucrează îndeaproape cu un program de rutare, examinează fiecare pachet de date din rețea (preluat fie din rețeaua internă – intranet, fie din rețeaua externă – Internet) ce trece prin rutor pentru a determina dacă va fi trimis sau nu mai departe spre destinație. Un firewall include de asemenea sau lucrează împreună cu un server proxy care face cereri de pachete în numele stațiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecție sunt instalate pe calculatoare ce îndeplinesc numai această funcție şi sunt instalate în fața rutoarelor.

Firewall-urile pot fi clasificate după:

- nivelul din stiva de rețea la care operează, în modelul ISO – OSI;
- modul de implementare.

În funcție de nivelul din stiva TCP/IP (sau OSI) la care operează, firewall-urile pot fi:

- Nivel 2 (MAC) şi nivel 3 (datagram): packet filtering;
- Nivel 4 (transport): tot packet filtering, dar se poate diferenția între protocoalele de transport (TCP şi UDP) şi există opțiunea de "stateful firewall", în care sistemul ştie în orice moment care sunt principalele caracteristici ale următorului pachet aşteptat, evitând astfel o întreagă clasă de atacuri;
- Nivel 5 (application): application level firewall (există şi alte nume). În general se comportă ca un server proxy pentru diferite protocoale, analizând şi luând decizii pe baza cunoştințelor despre aplicații şi a conținutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat application firewall pentru e-mail.

Deşi nu este o distincție prea corectă, firewall-urile se pot împărți în două mari categorii, în funcție de modul de implementare:

- dedicate, în care dispozitivul care rulează software-ul de filtrare este dedicat acestei operațiuni şi este practic "inserat" în rețea (de obicei chiar după rutor). Are avantajul unei securități sporite.
- combinate cu alte facilități de rețea. De exemplu, rutorul poate servi şi pe post de firewall, iar în cazul rețelelor mici acelaşi calculator poate juca în acelaşi timp rolul de firewall, rutor, file/print server etc.

Unul din cele mai bune firewall-uri este disponibil nativ pe kernel-ul Linux, fiind extrem de performant şi extrem de configurabil, permițând manipularea şi filtrarea pachetelor IP la majoritatea nivelelor OSI, în versiunile actuale chiar şi la nivel de aplicație. Uneori configurarea firewall-ului este greşit făcută, ducând la rezultate destul de imprevizibile în funcționare şi la deschiderea unor breşe de securitate destul de serioase. Tocmai de aceea se recomandă utilizarea unui utilitar care să scrie corect regulile şi mai ales în ordinea importanței acestora, aceasta fiind una din greşelile frecvente făcute de administratori. Unul din utilitarele cele mai bune şi uşor de configurat este NARC (NerFilter Automatic Rule Configurator), care permite implicit un aşa numit "Host LockDown". Host LockDown reprezintă de fapt o stare în care firewall-ul este complet neaccesibil ca sistem în rețea. Practic nu sunt acceptate nici un fel de conexiuni externe. După ce sistemul este adus în starea LockDown, se începe configurarea prin

deschiderea doar a porturilor necesare accesului extern, prin reconfigurarea aplicației.

NARC se instalează foarte uşor, având un script de configurare adaptat diferitelor versiuni Linux.

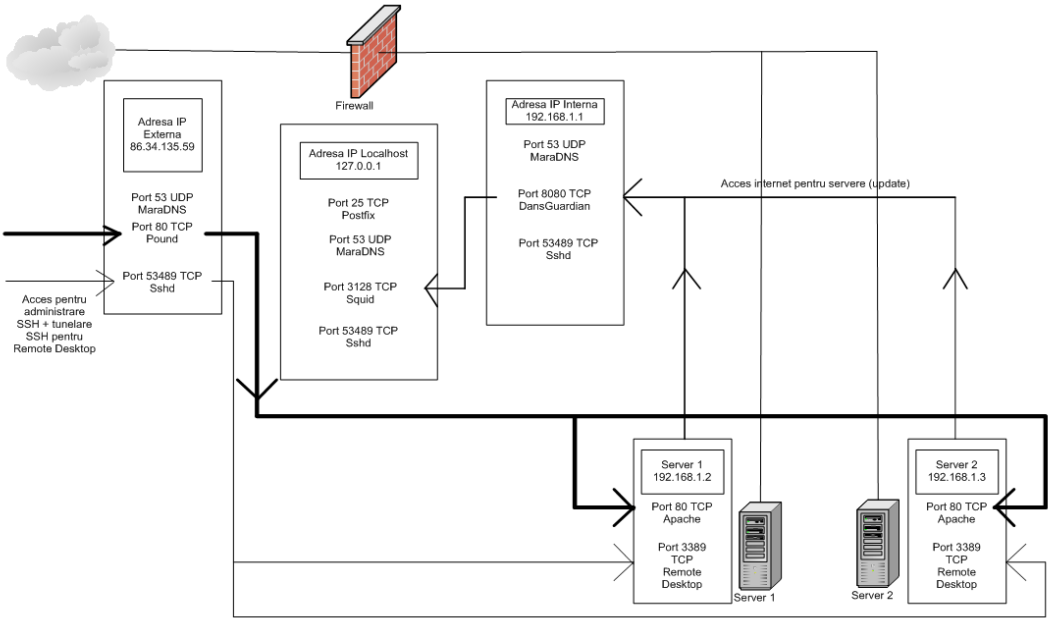

Figura 3. Schema de securitate a portalului MEDUCA

2.3 Securizarea accesului la portal şi distribuția încărcării prin aplicația POUND

Accesul la paginile web din portal nu se face direct pe serverul Apache ce găzduieşte aceste pagini. În sistemul firewall există o aplicație care verifică corectitudinea pachetelor HTTP, ulterior trimițând cererile către Serverul Web din rețeaua internă. Astfel se elimină posibilitatea ca un atacator să obțină drepturi direct pe sistemul care conține portalul, reducând foarte mult impactul unei astfel de acțiuni asupra securității în general. Această aplicație se numeşte **Pound**. Pound funcționează şi ca un mecanism de tip Load Balancer, adăugând portalului disponibilitate, în cazul în care unul din serverele backend nu mai este disponibil. Dacă cele două servere suport sunt funcționale atunci cererile clienților de acces la portal sunt în acest fel distribuite uniform pe cele două servere ce găzduiesc conținutul portalului.

Pound reprezintă o soluție open source Reverse Proxy fără cerințe hardware speciale. Această aplicație permite printre altele balansarea încărcării web front-end pe mai multe servere web backend. Dezvoltat de o companie de securitate IT, Pound este construit în ideea securității. Pound poate utiliza expresii regulate pentru a trimite cererile către servere back-end în funcție de headerul HTTP.

Pound este distribuit în licența GNU şi poate fi utilizat fără plată chiar şi în medii bussiness.

2.4 Implementarea şi securizarea serviciului DNS al portalului MEDUCA

Construit având la bază principii de securitate, MaraDNS reprezintă soluția optimă pentru implementarea unui server DNS în medii în care cerințele de securitate sunt extrem de stricte. Multitudinea de opțiuni pe care aplicația o aduce permite securizarea completă a serverului DNS din toate punctele de vedere.

Având în vedere că firewall-ul va trebui să conțină şi zona primară **meduca.ro** pentru serverul DNS al rețelei MEDUCA, implementarea soluției MaraDNS securizează accesul la

această informație publică. Zona DNS trebuie protejată pentru ca un eventual atacator să nu obțină informații despre structura rețelei portalului, informații ce i-ar permite să exploateze diferite zone ale portalului Web.

Configurarea MaraDNS trebuie făcută în două puncte distincte: configurarea serverului DNS şi configurarea zonei DNS.

Adăugarea serviciului DNS pe maşina firewall creşte într-o anumită măsură aria de expunere la atacuri externe. O reducere a acestui risc se poate face prin implementarea acestui serviciu într-o maşină virtuală separată.

2.5 Configurările de securitate pentru administrarea de la distanță a infrastructurii IT a portalului MEDUCA

Accesul pentru administrarea sistemului se realizează în totalitate ținând cont de condițiile de securitate impuse.

Astfel, pentru administrarea firewall-ului se foloseşte serviciul SSH, care criptează conexiunile şi asigură o securitate totală.

SSH sau Secure Shell este un protocol care permite schimbul de date între două sisteme pe un canal securizat. Utilizat în principal în medii Linux şi Unix, SSH-ul a fost dezvoltat ca un înlocuitor pentru Telnet şi alte metode de conectare remote nesigure, care permiteau trimiterea informațiilor într-un format necriptat, permițând unui atacator să valorifice informațiile captate, mai ales parole.

SSH utilizează o metodă criptografică bazată pe o pereche compusă dintr-o cheie de criptare publică şi o cheie de decriptare privată, permițând autentificarea clientului de către server, dar şi a serverului de către client, eliminând Spoofing-ul (înlocuirea identității serverului).

În cazul nostru serviciul SSH nu este disponibil pe portul standard, TCP 22, ci a fost mutat pe un port aleator desemnat, reducând posibilitatea accesului la acest serviciu în cazul unei scanări de porturi a unui utilizator extern rău intenționat.

De asemenea SSH-ul permite tunelarea şi criptarea completă a unor porturi locale de pe sistemul client (sistemul de administrare remote) spre porturi disponibile în rețeaua internă a portalului în vederea accesului la administrarea serverelor Windows, reducând eventualele probleme de securitate în cazul în care porturile Remote Desktop ale Windows-ului ar fi fost expuse în Internet.

Pentru accesul la funcția de administrare a portalului (a serviciilor web şi sql) disponibile pe Windows se foloseşte protocolul RDP (Remote Desktop Protocol), utilizând pentru deschiderea de sesiune un cont proiectat şi configurat să permită accesul complet la configurarea şi administrarea serviciilor Apache şi MySql. Directoarele în care sunt instalate aceste servicii sunt accesibile pentru acest utilizator, nefiind nevoie de accesul la alte zone ale sistemului de operare.

2.6 Scanarea, verificarea şi accelerarea accesului la conținutul paginilor Web

DansGuardian reprezintă o soluție performantă de scanare şi verificare a conținutului paginilor web pentru a limita accesul utilizatorilor la site-urile web cu conținut malițios. DansGuardian este instalat pe Linux sau Unix, extinzând capacitatea serverelor Proxy în filtrarea conținutului Web.

Arhitectura DansGuardian permite următoarele tipuri de filtrări:

- scanare antivirus cu ajutorul **ClamAv**, având integrat modulul de conectare la motorul antivirus;
- liste ale site-urilor web la care nu se permite accesul;
- liste cu URL-uri la care nu se permite accesul;

- mecanisme numite “advanced phrase weighting” folosite la identificarea tipului de conținut al paginilor web şi limitarea accesului la acele pagini care conțin foarte multe cuvinte blocate;
- limitarea accesului la anumite fişiere în funcție de extensia acestora.

Configurația de bază este extrem de restrictivă, fiind nevoie de ajustări ulterioare, pentru a permite accesul la anumite site-uri cu caracter public verificate.

DansGuardian nu face salvarea paginilor scanate, funcție a unui Proxy Server. În general poate folosi orice tip de server proxy, dar în majoritatea situațiilor este utilizat în comun cu **Squid Cache Proxy**. Configurări de securitate pot fi făcute şi în acest proxy server, putând să definim liste cu serviciile pe care le permitem şi sisteme de la care se acceptă conexiuni.

Serverul Squid Proxy este folosit pentru filtrare suplimentară, dar principalul său scop este acela de a accelera traficul web din rețeaua locală. Fiind un cache proxy, Squid salvează paginile folosite în sistemul de fişiere, ulterior, în cazul unei cereri asemănătoare poate să transfere fişierul respectiv direct clientului, fără a mai fi necesară aducerea acestuia din Internet. Dimensiunea zonei în care se poate face salvarea paginilor accesate este configurabilă, permițând o granularitate destul de bună.

Squid permite definirea de ACL-uri, pentru a configura cine şi la ce tip de acces are dreptul prin proxy. Pentru a securiza însă accesul la acest serviciu, portul disponibil pentru acces este pe 127.0.0.1. Conexiunea DansGuardian cu serverul Proxy Squid se face pe interfața locală 127.0.0.1, eliminând posibilitatea ocolirii DansGuardian.

Scanarea paginilor web se face cu ajutorul motorului antivirus ClamAV, integrat în DansGuardian, fără a mai fi nevoie de aplicația ClamAV instalată, ci doar de LibClamAV, o bibliotecă de proceduri apelabile de orice aplicație, implementabile prin ClamAV SDK. Actualizarea motorului antivirus se face doar cu instalarea unei noi versiuni ClamAV. În schimb, actualizarea bazei de date cu amprente de viruşi se face cu ajutorul FreshClam, care la intervale regulate de timp configurabile le aduce din Internet.

3. Concluzii

Modelul cadru pentru tehnologiile şi componentele unei soluții eLearning [8], ne-a permis o abordare arhitecturală a unui sistem eLearning, inclusiv a portalului ce trebuie proiectat şi realizat prin acest proiect. Acelaşi model cadru a fost folosit pentru aplicarea unei strategii globale de securizare a accesului utilizatorilor la serviciile oferite de portalul MEDUCA.

Configurările de securitate pe infrastructura IT software au fost implementate:

1. direct pe infrastructura IT software oferită de servere, echipamentul de stocare şi rețeaua fizică, iar în faza următoare a proiectului aceste configurări vor fi redefinite.

2. Pe o infrastructură de maşini virtuale create pe infrastructura IT hardware în concordanță cu nevoile de securitate şi performață ale proiectului MEDSCEN. Această soluție ne oferă mai multă securitate, prin reducerea suprafețelor expuse la atacuri dinspre Internet.

BIBLIOGRAFIE

1. **BEVANDA,V., J. AZEMOVIC, D. MUSIC,** Privacy Preserving in eLearning Environment (Case of Modeling Hippocratic Database Structure), Proceedings of the 2009 Fourth Balkan Conference in Informatics, 2009, pp. 47-52.
2. **RAITMAN, R., L. LEANNE NGO, N. AUGAR,** Security in the Online E-Learning Environment, Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies, 2005, pp. 702 – 706.

3. **FRANZ, E., H. WAHRIG, A. BOETTCHER, K. BORCEA-PFITZMANN,** Access Control in a Privacy-Aware eLearning Environment, Proceedings of the First International Conference on Availability, Reliability and Security, 2006, pp.879 – 886.

4. **SADEGHI, A. R., C**. **STÜBLE,** Towards multilaterally secure computing platforms-with open source and trusted computing, Information Security Tech. Report, Volume 10 , Issue 2 (January 2005), pp. 83-95.

5. **JALAL, A., M. A. ZEB,** Security Enhancement for E-Learning Portal, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008, pp. 41-46.

6. http://medscen.expert.org.ro/

7. http://www.meduca.ro/

8. **ROCEANU, I.** coord., Proiectarea şi realizarea sistemului integrat eLearning pentru servicii educaționale on-line, Editura Universitară, Bucureşti, 2008.