TEHNIKA I INFORMATIKA U OBRAZOVANJU
5. Konferencija sa međunarodnim učešćem, FTN Čačak, 30–31. maj 2014.
TECHNICS AND INFORMATICS IN EDUCATION
5th International Conference, Faculty of Technical Sciences Čačak, 30–31th May 2014

UDK: 37.018.43 Stručni rad

PRAĆENJE KAO ELEMENT BEZBEDNOSNE ARHITEKTURE SISTEMA ZA E-UČENJE[1]

Marjan Milošević[2], Danijela Milošević[3]

***Rezime**: Bezbednost informacija usko je povezana sa svim sferama korišćenja informaciono-komunikacionih tehnologija. Kako e-učenje postaje sve prihvaćeniji model obrazovanja i u formalnom i u neformalnom obliku, pojavljuje se potreba za sistematičnim pristupom bezbednosti informacija u sistemima e-učenja. Kompleksnost procesa koji se odvijaju u e-učenju zahteva kreiranje namenskog modela i odgovarajuće prilagođene arhitekture. U radu je prikazan jedan pristup takvoj arhitekturi, sa predlozima za implementaciju, uz poseban naglasak na modul za praćenje.*

***Ključne reči:** e-učenje, bezbednosna arhitektura, bezbednost informacija, Moodle.*

MONITORING AS AN ELEMENT OF INFORMATION SECURITY ARCHITECTURE OF E-LEARNING SYSTEMS

***Summary**: Information security is tightly connected to all areas of ICT usage. As e-learning model is getting wider acception in both formal and non-formal form, there is a need for a sytematic approach to information security in e-learning systems. The complexity of processes conducted in e-learning requires creation of a special model and adequate adapted architecture. The paper presents an approach to this kind of architecture, with implementation suggestions, with a special emphasis on monitoring module.*

***Key words:** e-learning, information security architecture, information security, Moodle*

[1] *Rad je razvijen u okviru projekta "Infrastruktura za elektronski podržano učenje u Srbiji" III 47003 koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije, a nosilac je FON Beograd*

[2] *Mr Marjan Milošević, Fakultet tehničkih nauka u Čačku, Univerzitet u Kragujevcu, e-mail: marjan.milosevic@ftn.kg.ac.rs*

[3] *Dr Danijela Milošević, Fakultet tehničkih nauka u Čačku, Univerzitet u Kragujevcu, e-mail: danijela.milosevic@ftn.kg.ac.rs*

1. UVOD

Društvo znanja i Internet-era predstavljaju prirodan ekosistem za razvoj e-učenja. U tom smislu evidentan je porast različitih različitih oblika e-učenja u sklopu formalnog i neformalnog obrazovanja. Procenjuje se da je e-učenje trenutno "teško" preko 56 milijardi dolara, a da će se ta cifra udvostručiti za manje od dve godine [1].

E-učenje neretko je na meti kritika kojima su na udaru konkretno metode nastave, ali i organizacioni elementi [2]. U poslednje spada upravo oslonjenost na tehnologiju, koja sa sobom povlači i pitanja bezbednosti podataka koji se koriste u e-obrazovanju, a koji su u potpunosti oslonjeni – po pitanju stvaranja, izmene i čuvanja - na informacione tehnologije. U tom smislu postoji potreba da se ovi infrastrukturni elementi takođe urede, što podrazumeva procedure, dokumentaciju, odnosno odgovarajuću softversku podršku.

Bezbednost je definisana kao multidisciplinarni koncept, a upravljanje bezbednošću zahteva inovativan pristup, s obzirom na složenost modernih informacionih sistema i raznovrsnost napada i zloupotreba. U tom smislu imperativ je razvijanje sveobuhvatnog, holističkog modela, koji uzima u obzir raznovrsne faktore od značaja za bezbednost. Na taj način omogućava se sistematična realizacija odgovarajućih kontrola (mehanizama i procedura zaštite) i formira okvir za konstantno unapređenje bezbednosti uticajem na sve relevantne kategorije od kojih ona zavisi.

Svaki prekid u radu, gubljenje podataka, narušavanje privatnosti ili pad performansi direktno utiče na kvalitet učenja, ali i kompromituje samu obrazovnu instituciju. Stoga je od naročitog značaja zaštititi sistem i smanjiti verovatnoću otkaza i narušavanja bezbednosti.

Ovakav cilj je moguće ostvariti izgradnjom odgovarajuće bezbednosne arhitekture - ISA (Information Security Architecture).

2. BEZBEDNOSNA ARHITEKTURA

Bezbednosna arhitektura (ISA – Information Security Architecture) se definiše kao proces razvoja svesnosti o rizicima, provere postojećih kontrola i usklađenosti postojećih i novih kontrola sa bezbednosnim ciljevima organizacije [3]. ISA je upravljački proces usmeren ka postizanju i održavanju bezbednosnih servisa kao što su npr. autentifikacija i autorizacija.

2.1. Opšti modeli bezbednosnih arhitektura

U literaturi se mogu pronaći raznovrsni modeli bezbednosnih arhitektura informacionih sistema. Istraživači, praktičari i bezbednosni eksperti su pokušali da osvetle pitanje bezbednosti kroz holistički pristup. Poenta holističkog pristupa je da što kompletnije, na određenom visokom nivou apstrakcije, obuhvati različite aspekte koji utiču na bezbednost. U tom smislu važno je akcentovati i činioce koji su ne-tehničke prirode, na primer. bezbednosnu kulturu.

Standardizovani model 27001 oslanja se na PDCA ciklus i razmatra bezbednost kao kružni neprekidni proces [4].

Pristup sličan ISO-u dali su i Ris i dr. u svom PFIRES modelu [5]. PFIRES je prvobitno bio namenjen elektronskoj trgovini, ali je kasnije proširen. Osnovu nalazi u ciklusu razvoja proizvoda i softvera. Model predviđa kratkoročne ciljeve, koji su operativni i razrađeni do dnevnog nivoa i dugoročne strategije, koje zahtevaju ozbiljnije uključivanje višeg menadžmenta.

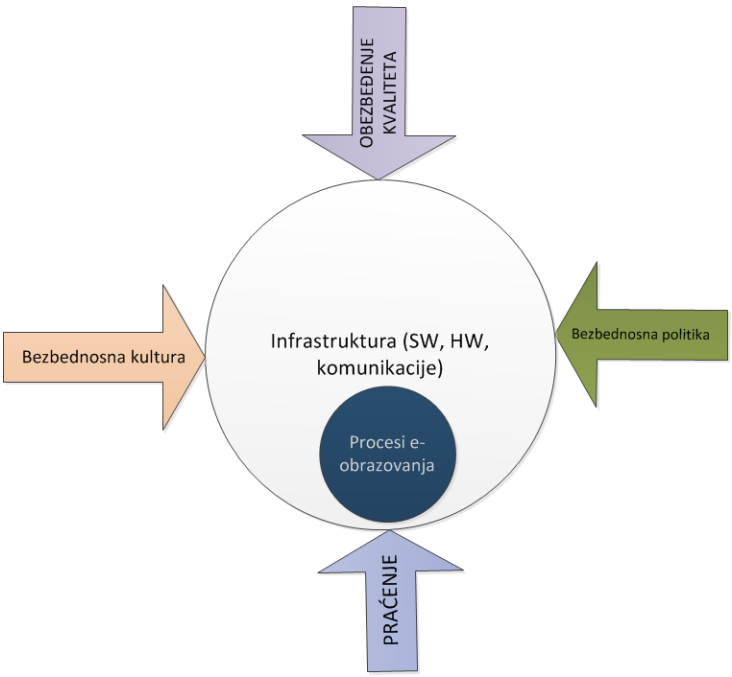
Tjudorov pristup ilustrovan je slikom 1:

Slika 1: *Bezbednosna arhitektura (Tjudor[2])*

Trček predlaže višedimenzioni model koji integriše više postojećih pristupa [6]. Prvi horizontalni nivo bavi se interakcijom čovek-računar i vodi ka ostalim ravnima ispod, koji se bave fizičkom bezbednošću i servisima kao što je kriptografija na nižim nivoima.

MekKamber je razvio istoimenu kocku bezbednosti, koja takođe ima za cilj integraciju različitih aspekata bezbednosti [7].

SeLMa model bezbednosti u e-obrazovanju [8] predstavlja jedan pristup razvoju arhitekture kojim se postižu ciljevi bezbednosti u multidisciplinarnom maniru, kakav se zahteva u domenu e-učenja.



Slika 2: *SeLMa model arhitekture*

2.2. Elementi bezbednosnog modela

Infrastruktura podrazumeva sve programske i fizičke elemente (hardver i softver) koji predstavljaju logistiku procesa e-obrazovanja.

Procesi e-učenja su svi biznis-procesi koji se odvijaju u sklopu e-učenja: npr. upis kursa, postavljanje domaćeg zadatka, unos u viki-strane.

Bezbednosna kultura i svest (awareness) zauzimaju posebno mesto u modelu. Edukacija, formiranje svesti o značaju bezbednosti i bezbednosnoj kulturi ima uticaj na različitim nivoima bezbednosti: od fizičkog do logičkog, odnosno na sve elemente bezbednosne trijade (CIA). Kako je pokazano u studiji slučaja [8], postoji niz indikatora da je bezbednosna svest kod korisnika (e-učenika) na nezavidnom nivou, a takođe su sami korisnici ustanovili potrebu za sopstvenom edukacijom u ovoj oblasti.

Obezbeđenje kvaliteta može se posmatrati kao ulazni, ali i izlazni proces. Za sistem čiji se kvalitet proverava moraju se prvo ustanoviti potrebe kvaliteta, implementirati traženi zahtevi i standardi, čime samo obezbeđenje kvaliteta predstavlja faktor ulaza u proces izgradnje bezbednosnog modela i njegove implementacije. Po formiranju okruženja kod kojeg su primenjeni kriterijumi osiguranja kvaliteta, vrši se evaluacija i u tom slučaju je sam element e-učenja ulaz u procesu evaluacije.

Praćenje podrazumeva konstantno prikupljanje povratnih informacija, evidentiranje aktivnosti i svih propratnih informacija koje mogu biti od značaja za procese unapređenja postojećeg modela. Praćenjem se konstantno dobijaju informacije na osnovu kojih se preduzimaju određene akcije, odnosno koje govore o stepenu uspešnosti trenutnih kontrola.

Legislativa i bezbednosna politika predstavljaju formalne faktore u čijim okvirima se realizuju bezbednosni ciljevi. Zakonski okviri o očuvanju informacija su definisani odgovarajućim zakonskim i podzakonskim aktima i bilo kakav informacioni sistem, pa i sistem e-obrazovanja mora biti usklađen sa odgovarajućim propisima. Procedure predstavljaju sistematizovanu formalizaciju internih oblika ponašanja. Npr. procedura u slučaju kompromitovanja lozinke ili pronalaženja virusa. Osnovni dokument koji figuriše je bezbednosna politika, kojom se razumljivim jezikom definišu bezbednosni ciljevi. Bezbednosna politika zapravo je srž, doktrina oko koje se dalje formiraju ostali elementi.

3. PRAĆENJE KAO ELEMENT BEZBEDNOSNE ARHITEKTURE

Bezbednosno praćenje samo po sebi nije bezbednosna kontrola, odnosno ne predstavlja meru zaštite od određenih, identifikovanih oblika napada, već se definiše kao konstantno praćenje događaja koji su od značaja za procese koji se odvijaju u organizaciji [9]. U praksi postoje različite komponente informacionog sistema i bezbednosno praćenje podrazumeva prikupljanje što većeg broja relevantnih informacija koje proističu iz rada tih komponenti.

Kod sistema e-učenja praćenje se može vršiti na različitim nivoima:

- na organizacionom nivou: praćenje poštovanja procedura, npr. ko može da otvori nove kurseve i u skladu sa kojim regulativama,
- na nivou sistema za upravljanje e-učenjem: praćenje pristupa, aktivnosti aplikacije, servera itd.

Kada je reč o praćenju u sklopu sistema za upravljanje e-učenjem, postoje različiti mehanizmi pomoću kojih se – na različitim slojevima softverske platforme – mogu generalno pratiti aktivnosti. Samo okruženje za e-učenje (npr. Moodle) poseduje svoje mehanizme za praćenje aktivnosti, beleženje u odgovarajuće dnevnike i obaveštavanje o

nekim osnovnim bezbednosnim događajima. Ovim dnevnicima mogu pristupati u određenoj meri svi korisnici i uglavnom služe za praćenje napredovanja učenika, pristup određenim sadržajima i dobijanje statistike na nivou kursa ili čitavog sajta. Sa druge strane, ovakvi zapisi mogu se koristiti i u funkciji bezbednosnog praćenja, fokusiranjem na određene parametre koji su za tu svrhu relevantni, npr. učestalost određenih akcija, postavljanje specifičnih sadržaja, problemi sa pristupom itd.

3.1 Ugrađeni mehanizmi za praćenje – na primeru Moodle LMS

Moodle predstavlja široko zastupljen LMS otvorenog koda, sa više od 85000 registrovanih instalacija u 240 zemalja [10].

Podrazumevani način praćenja aktivnosti korisnika je beleženjem akcija u posebnu tabelu. Zapis sadrži informacije o tipu akcije i korisniku (slika 3).

E-Učenje: Marjan Milošević, Četvrtak, 24. April 2014. (Europe/Belgrade)

E-Učenje (Sajt) | Marjan Milošević | Četvrtak, 24. April 2014. | Sve aktivnosti | Sve akcije | Prikaži na stranici

Preuzmi ove zapise o aktivnostima

Prikaz 13 zapisa

Kurs	Vreme	IP adresa	Puno ime korisnika	Akcija	Informacija
eup	Čet 24. April 2014., 12:56	91.187.132.18	Marjan Milošević	quiz continue attempt	E-Test
eup	Čet 24. April 2014., 12:56	91.187.132.18	Marjan Milošević	quiz view	E-Test
eup	Čet 24. April 2014., 12:55	91.187.132.18	Marjan Milošević	course view	Eucenje-proba
eup	Čet 24. April 2014., 12:55	91.187.132.18	Marjan Milošević	course view	Eucenje-proba
eup	Čet 24. April 2014., 12:55	91.187.132.18	Marjan Milošević	course view	Eucenje-proba

Slika 3: *Pregled dnevnika događaja (Moodle)*

Beleženje dnevničkog zapisa vrši se iz osnovnog sistema, odnosno iz dodataka (plaginova) putem odgovarajućih API poziva funkcija. Otvorenost kôda Moodla pruža mogućnost postavljanja odgovarajućih poziva u module sistema čije se dodatno praćenje iziskuje, odnosno dopunjavanja postojećih poziva dodatnim relevantnim informacijama, koji bi mogli pomoći u otkrivanju bezbednosnih anomalija i neželjenog ponašanja. U verziji 2.5 uveden je koncept događaja, koji će dalje omogućiti kompletniji, sistematičniji i skalabilniji način beleženja dnevničkih zapisa [11].

Moodle pruža osnovne statičke mogućnosti za dobijanje informacija o aktivnostima korisnika, vraćajući rezultate upita prema vremenu, korisniku, kursu i sl.

3.2 UPRAVLJANJE BEZBEDNOSNIM INFORMACIJAMA I DOGAĐAJIMA

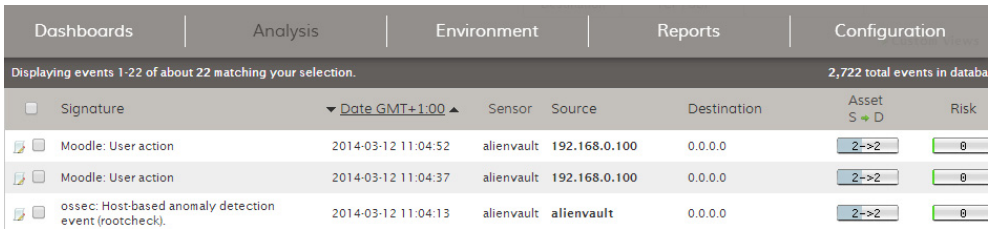
Složenost sistema iziskuje beleženje brojnih informacija i pri tome treba voditi računa i o resursima koje ovo beleženje zahtevaju: prostoru na disku, opterećenju procesora i mreže itd. Pri praćenju se zapisi čuvaju u raznorodnim formatima, što može predstavljati izazov ukoliko je potrebno izvršiti analizu ili tražiti relaciju među zapisima. U tu svrhu čest izbor je korišćenje alata za upravljanje bezbedosnim informacijama i događajima (SIEM / security information and event management), kao i namenskim alatima za analizu

dnevničkih (log) zapisa. SIEM integriše različite alate za praćenje i detekciju i administratoru olakšava centralizaciju podataka koji se prikupljaju iz brojnih izvora.

Rešenja poput SIEM generalno mogu biti od pomoći u praćenju bezbednosnih informacija, kao i usaglašenosti sa regulativama kroz aktivnosti kao što su:

- agregacija i normalizacija podataka o događajima sa različitih nezavisnih uređaja, servisa i aplikacija i formiranje upotrebljivih informacija,
- analiza i korelacija informacija iz različitih izvora kao što su: skeneri ranjivosti, IDS/IPS (sistemi za detekciju i prevenciju upada), zaštitne barijere (fajervol), serveri itd, radi identifikacije napada što pre je to moguće i što brže reakcije na upad,
- sprovođenje forenzičke analize mreže na osnovu istorije ili podataka u realnom vremenu kroz vizualizaciju i ponavljanje događaja,
- kreiranje prilagođenih izveštaja radi bolje vizualizacije bezbednosne slike organizacije
- povećanje efikasnosti osoblju zaduženom za upravljanje rizicima,
- usaglašavanje sa regulativama i forenzičkim zahtevima za bezbedno i dugoročno čuvanje podataka o svim događajima i trenutan pristup arhiviranim podacima.

Primer SIEM platforme otvorenog kôda je OSSIM [12]. U pitanju je softver zasnovan na Linuxu koji u sebi integriše raznovrsne servise za prikupljanje podataka i, što je jako važno, korelaciju. OSSIM poseduje veliki broj dodataka (pluginova) koji omogućavaju prikupljanje dnevnika iz najraznovrsnijih izvora. Tako postoji i rudimentarna varijanta Moodle dodatka, pomoću kojeg se preuzimaju standardni Moodle logovi. Na slici 4 prikazan je izgled interfejsa za praćenje događaja u OSSIM-u.



Slika 4: Analiza događaja u OSSIM-u

Korisna opcija OSSIM-a je upravo otvorenost kôda koja omogućava pisanje prilagođenih dodataka i doradu postojećih. Autori su u samim dodacima standardizovali polja podataka koji se prikupljaju sa tzv. Senzora, ostavljajući pri tome nekoliko polja za slobodnu upotrebu, dajući time dodatnu fleksibilnost u korišćenju.

4. ZAKLJUČAK

Trendovi u informatičkoj industriji se ukrštaju sa putevima modernog obrazovanja. Na toj raskrsnici nezaobilazni su izazovi bezbednosti. Uz odgovarajući pristup i konsultovanje postojećih modela, izgrađena je arhitektura koja može poslužiti kao dobra konceptualna osnova za implementaciju bezbednosnih mehanizama. U tom sklopu praćenje predstavlja jednu od vitalnih aktivnosti, koja je preduslov za aktiviranja mehanizama zaštite i „okretanje“ kruga kvaliteta.

Sistemi za upravljanje učenjem već poseduju određene mogućnosti praćenja aktivnosti, koji se mogu iskoristiti za potrebe regulisanja nastave, dobijanje trendova učenja i slično, ali i u svrhe bezbednosnog praćenja. Ove mogućnosti su ograničene i potrebno ih je obogatiti

opcijama koje su posebno namenjene bezbednosti. Takođe, za efikasno korišćenje dnevnika, potrebno je izgraditi mehanizme za analizu zapisa i traženje odgovarajućih šablona.

Za celovito praćenje, na više nivoa softverske platforme, pored ugrađenih mogućnosti, na raspolaganju su rešenja koja objedinjuju prikupljanje i analizu podataka iz različitih izvora. Postavljanjem ovakvih, SIEM platformi, dobija se poseban servis koji je namenjen praćenju aktivnosti softverske platforme i, zajedno sa ugrađenim mogućnostima, predstavlja kompletiran modul za praćenje kao delo bezbednosne arhitekture sistema za e-učenje.

Zaokružen modul bezbednosnog praćenja podrazumeva prilagođavanje postojećih metoda, koje su ugrađene u samoj platformi i integraciju sa drugim izvorima informacija primenom odgovarajućeg sistema za upravljanje bezbednosnim informacijama i događajima (SIEM). Rešenja otvorenog kôda se nameću kao logična usled mogućnosti izmene izvornog programa i kreiranja adaptiranog rešenja za potrebe sistema za e-učenje.

Budući rad podrazumeva implementaciju modula arhitekture u realnom sistemu i evaluaciju njegovog rada.

5. LITERATURA

[1] ***, E-Learning magazine (2013) http://elmezine.epubxp.com/t/67167_pp10 *sep2013,* (posećeno aprila 2014)

[2] Tudor, JK (2000). Information Security Architecture, Taylor And Francis

[3] Butler, D.L., Selborn M. (2002). Barriers to adopting technology for teaching and learning, Educause quarterly, No2, https://net.educause.edu/ir/library/pdf/eqm0223.pdf (posećeno aprila 2014)

[4] ***, ISO (2005) ISO/IEC 27001*,* Information technology — Security techniques — Information security management systems — Requirements, *ISO/IEC*

[5] Rees J, Bandyopadhyay, S., Spafford, EH (2003) PFIRES: A Policy Framework for Information Security, Communications of the ACM July 2003/Vol.46 (7) pp 101- 106.

[6] Trcek, D. (2003) An integral framework for information systems security management, Computers & Security, Vol. 22 (4), pp 337-360.

[7] McCumber, J. (2005) Assessing and Managing Security Risk in IT Systems: a Structured Methodology. Boca Raton, FL: Auerbach Publications

[8] Milosevic, M., Milosevic D, Krneta R. (2013): INFORMATION SECURITY IN E-LEARNING: THE MATTER OF QUALITY, Preceedings - The Fourth International Conference on e-Learning (eLearning-2013), 26-27 September 2013, Belgrade, Serbia pp 15 -19

[9] Vacca, J. (2009). Computer and information security handbook, Morgan-Kaufmann, Boston

[10] ***, Moodle Statistics, https://moodle.org/stats/ (posećeno aprila 2014)

[11] ***, Moodle Logging, http://docs.moodle.org/dev/Logging_2 (posećeno aprila 2014)

[12] ***, OSSIM: Open Source SIEM & Open Threat Exchange Projects, http://www.alienvault.com/open-threat-exchange/projects (posećeno aprila 2014)