

BEZBEDNOSNA ARHITEKTURA LOTUS DOMINO PLATFORME U INFORMACIONOM SISTEMU KRIMINALISTIČKO-POLICIJSKE AKADEMIJE

Mr Olga Stamatović-Đurić, *Kriminalističko-policijska akademija, Beograd,*
olgasdj@ptt.yu

Goran Bjelobaba, *Kriminalističko-policijska akademija, Beograd,*
gbjelobaba@gmail.com

Milena Lučić,
lenami24@yahoo.com

Apstrakt: U ovom radu se razmatra bezbednosni aspekt arhitekture Lotus Domino platforme u Informacionom sistemu Kriminalističko-policijske akademije. Izloženi su principi Domino modela zaštite koji podrazumeva skup mehanizama i preporuka za zaštitu resursa sistema. Pored osnovnog koncepta Domino modela zaštite, prikazana je i praktična primena datog modela tokom implementacije i korišćenja Informacionog sistema Kriminalističko-policijske akademije.

Ključne reči: informacioni sistem, zaštita, Lotus Domino

THE LOTUS DOMINO PLATFORM SECURITY ARCHITECTURE IN CRIMINAL-POLICE ACADEMY INFORMATION SYSTEM

Abstract: In this paper, security aspects of Lotus domino platform architecture in Criminal-Police Academy Information System are considered. The Domino security model principles, consisting of technique and recommendation set, intended for system resources security, are presented. In addition to Domino security model basic concepts, practical application of this model during implementation and usage in Criminal-Police Academy Information System is described.

Key words: information system, security, Lotus Domino

1. UVOD

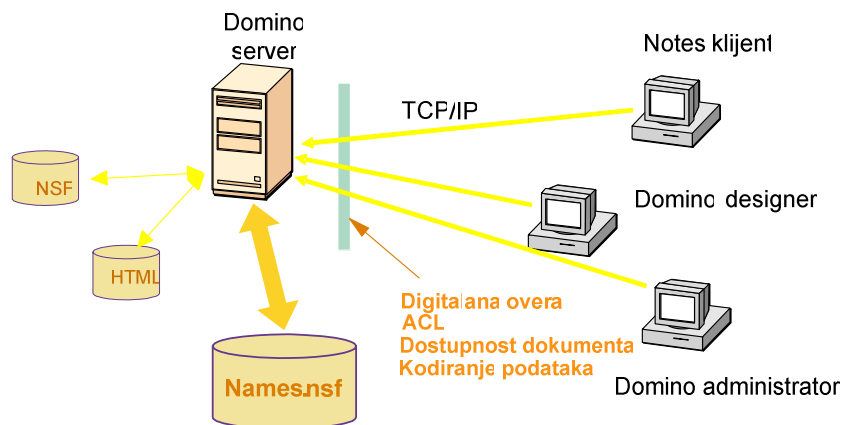
Stalni rast primene savremenih informacionih tehnologija u svim oblastima ljudskog života, a naročito u poslovnim sistemima, dodatno je ubrzan tokom protekle decenije. Ekspanzija Interneta i internet tehnologije u računarskim mrežama (intranet, extranet), doprinela je povećanju broja korisnika (kompanija i pojedinaca) različitih mrežnih usluga. Protok informacija postaje brži, a cena njihovog prenosa sve manja. Informacije u elektronskom poslovanju dobijaju kvalitativnu odrednicu – kapital (knowledge capital) i postaju podjednako značajne kao i finansijski kapital. Zbog toga i problematika njihove zaštite postaje sve kompleksnija. Broj napada na informacione sisteme i mogućnost odliva informacija iz godine u godinu progresivno rastu. Mogući uzroci ugrožavanja bezbednosti računarskih sistema klasifikovani su na različite načine kao bezbednosne pretnje. Zanimljivo je da različite analize učestalosti napada ukazuju da interni ljudski faktor (radnici poslovnog sistema), predstavlja dominantnu pretnju (80%). Od toga je 55% nenamernih napada, a 25% namernih. Preostalih 20% bezbednosnih incidenata raspodeljeno je, u zavisnosti od autora, na eksterni ljudski faktor, greške hardvera i softvera, prirodne i društvene katastrofe itd.

Veliki broj napada na informacione sisteme različitih poslovnih sistema (preduzeća, organa državne uprave...) primorao je mnoge IT kompanije na ulaganje novca i resursa u razvijanje sistema zaštite. IBM nudi rešenje problema degradacije, uništenja, neadekvatnog korišćenja i zloupotrebe podataka u vidu mehanizama zaštite, integrisanih u svoju Lotus Domino platformu. Lotus Notes / Domino je vodeća *client/server* arhitektura (IBM 49% tržišta, a Microsoft 39%) za collaborative messaging i e-business rešenja. Lotus Notes i Domino imaju ogromne mogućnosti ali njihov primarni cilj je da pruže jedinstvenu platformu za upravljanje podacima, a usmereni su na nivo radne grupe. Suština je u tome kako navesti ljude da rade zajedno, da razmenjuju i dele ideje i da učestvuju u timskom radu. Upotrebljavali se zajedno ili odvojeno, Notes i Domino omogućavaju efikasnost, efektivnost i fleksibilnost poslovanja.

2. DOMINO MODEL ZAŠTITE

Komponente client/server arhitekture Lotus Notes/ Domino su:

- Lotus Domino server- Enterprise server koji sadrži: Mail server, Application server i Web server
- Lotus Notes klijent
- Lotus Domino Designer
- Lotus Domino Administrator



Slika1. Lotus Domino arhitektura

Domino model zaštite predstavlja skup mehanizama i preporuka za zaštitu resursa sistema implementiranog na Lotus Domino platformi i obuhvata: fizičku zaštitu, zaštitu operativnog sistema, mrežnu zaštitu, zaštitu servera, ID bezbednost, zaštitu aplikacija, bezbednosni dizajn elemenata aplikacije i zaštitu podataka na radnoj stanici. Za resurse ili objekte koji se štite definisana su pristupna prava korisnika. Informacije o pravima pristupa sistemu i privilegijama uskladištene su sa svakim zaštićenim resursom. Shodno tome, određeni korisnik ili server mogu da imaju različiti skup prava pristupa, u zavisnosti od resursa kojima dati korisnik ili server pristupaju.

2.1 Fizička zaštita

Fizička zaštita [2] servera i baze podataka podjednako je važna kao i prevencija neovlašćenog pristupa lica serveru. To je prva linija zaštite koja sprečava direktan kontakt neautorizovanih i zlonamernih korisnika sa Domino serverima. Zbog toga se i preporučuje da se Domino serveri smeste u osigurane prostorije (restriktivni prostor) sa odgovarajućom ventilacijom. Ako serveri nisu fizički bezbedni, neautorizovani korisnici mogu da izbegnu zaštitne mehanizme kontrole pristupa, na primer ACL podešavanja i pristupe aplikacijama direktno na serveru. Pristup serveru omogućava kopiranje i uklanjanje podataka korišćenjem operativnog sistema, kao i fizičko oštećenje servera. Fizička zaštita treba da uključi i plan u slučaju prirodnih nepogoda.

2.2 Zaštita operativnog sistema

Neautorizovani i zlonamerni korisnici često povećavaju ranjivost operativnog sistema. Administrator sistema treba da osigura operativni sistem na kome je Domino server implementiran [2]. Na primer, potrebno je da se: ograniče administratorska prava prijavljivanja na operativni sistem; onemogući FTP (na NT); izbegava upotreba mapiranih kataloga na serveru datoteka. Administrator sistema mora stalno da prati bezbednosne ispravke nedostataka operativnog sistema (updates and patches) i redovno pregleda log datoteke.

2.3 Mrežna zaštita

U cilju bezbednosti računarske mreže, neautorizovanim korisnicima treba onemogućiti pristup serveru, korisnicima i podacima [2]. Fizička zaštita mreže mora biti postavljena pre nego što ostvarimo povezivanje klijenta i servera (Lotus Notes i Domino). Fizička zaštita mreže ostvaruje se korišćenjem sledećih uređaja: filtrirajući ruteri, mrežne barijere (firewall-ovi) i proxy serveri. Na taj način eliminiše se mogućnost konekcije na raznovrsne servise (LDAP, POP3, FTP i STMP).

Pomenuti uređaji sprečavaju da neautorizovani korisnik:

- neovlašćeno pristupi mreži, serveru i njegovom operativnom sistemu kao i njegovim servisima (kao što je file sharing);
- lažno se predstavi kao autorizovani Notes korisnik;
- prikuplja podatke prisluškivanjem na mreži.

2.4 Zaštita servera

Domino server je najkritičniji resurs za čuvanje i prvi je nivo zaštite koju Domino model preporučuje posle korisničkog i serverskog pristupa serveru na mreži [3]. Moguće je specifikovati koji korisnik i server može pristupiti serveru i ograničiti aktivnosti na serveru. Na primer, može se odrediti ko može da kreira novu kopiju i da koristi posrednu (pass-through) konekciju. U cilju ograničavanja administratorskog pristupa preporučuje se delegiranje pristupa zasnovanog na administratorskim zaduženjima i zadacima. Na primer, može se omogućiti pristup operativnom sistemu kroz serversku konzolu za sistem administratora i dozvoliti pristup bazi administratoru koji je zadužen za administriranje Domino baze. Korišćenje servera za Internet/intranet pristup zahteva podešavanje SSL, ID i lozinke. Ovim se ostvaruje identifikacija servera i klijenta neophodna za zaštitu protoka podataka preko mreže

2.5 ID bezbednost

Notes ili Domino ID jedinstveno određuje korisnika ili server [3]. Informacije sadržane u ID-u, Domino koristi za kontrolu pristupa korisnika ili servera prema drugim aplikacijama. Jedna od odgovornosti administratora je da zaštite ID i da obezbede da ih neautorizovani korisnici ne koriste kako bi dobili pristup Domino okruženju.

Pojedini sistemi mogu zahtevati od više administratora da saopšte lozinke pre dobijanja pristupa serverovoj ID datoteci. Ovo sprečava da samo jedna osoba ima pristup ID datotekama.

Dodatna zaštita Notes korisničkog ID-a, može se obezbediti upotrebom inteligentnih kartica. Smartkartice smanjuju opasnost od korisničkih ID prevara, tako što se proverava identitet korisnika na osnovu ID, potom pomoću smartkartice, a pristup Notes-u se dozvoljava nakon unosa PIN-a smartkartice.

2.6 Zaštita aplikacija

U cilju ograničavanja pristupa koji korisnik i serveri imaju na određenoj Domino aplikaciji na serveru, nakon prvog pristupa korisnika i servera Domino serveru, omogućen je bazni pristup Listama za kontrolu pristupa (ACL). U kontekstu obezbeđenja pri-

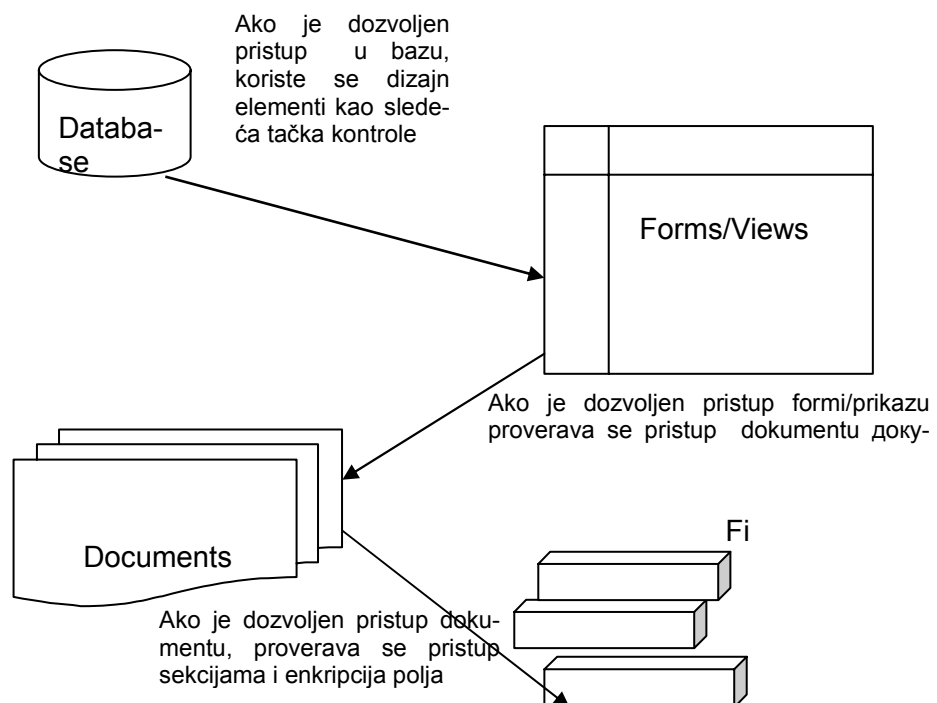
vatnosti podataka, vrši se enkripcija baze sa ID-om, tako da neautorizovani korisnici ne mogu pristupiti lokalno smeštenoj kopiji datoteke [5].

Pristupni nivoi prijavljenih korisnika u bazi ACL definišu koji zadatak korisnik može da izvede u bazi. Svaka baza ima svoj pristupni kontrolni list baze (ACL) koji određuje nivo pristupa koji svaki korisnik i server ima na datoj bazi. Iako su imena pristupnog nivoa ista kod korisnika i servera, oni koji su prijavljeni kao korisnici određuju koje će poslove obavljati u bazi, dok oni koji su prijavljeni na server određuju koje informacije unutar baze, server može replicirati. Samo osoba sa najvećim ovlašćenjima pristupa (Manager access) može da formira i modifikuje ACL.

Da bi se kontrolisala pristupna prava Notes korisnika, dodeljuje im se: pristupni nivo, tip korisnika, pristupni nivo privilegija za svakog korisnika ili grupu u bazi. Mogu se podesiti preporučeni (default) ulazi u ACL kada se kreira baza. Za svakog korisnika, grupu ili serversku listu u ACL, odabira se osnovni pristupni nivo i korisnički tip (basic access level and user type). Pre formiranja baze, potrebno je isplanirati pristupni nivo za sve korisnike u saradnji sa dizajnerima i korisnicima aplikacije.

2.7 Bezbednosni dizajn elemenata aplikacije

Korisnik može imati pristup aplikaciji, ali ne i svim projektovanim elementima aplikacije. Može se ograničiti pristup pojedinim elementima aplikacije – na primer: forme, prikazi (views) i folderi. Kada projektuje Domino aplikaciju, razvojni inženjer može koristiti pristupni list i specijalna polja da ograniči pristup specifičnim elementima dizajna [5].



Slika2. Bezbednosna arhitektura Lotus Domino okruženja

2.8 Zaštita podataka na radnim stanicama

Notes korisnici mogu držati i koristiti važne aplikacije i informacije na svojim radnim stanicama [4]. Ove informacije mogu biti zaštićene upotrebom izvršne kontrolne liste (ECL), koja definiše pristup aktivnom sadržaju drugih korisnika.

3. INFORMACIONI SISTEM KRIMINALISTIČKO-POLICIJSKE AKADEMIJE (KPA)

3.1. Struktura Informacionog sistema KPA

Informacioni sistem KPA razvijen je u Višoj školi unutrašnjih poslova kao rezultat planskog nastojanja da se unapredi obrazovno-vaspitna delatnost i poslovanje obrazovnih institucija Ministarstva unutrašnjih poslova. Strategijski plan dugoročnog razvoja informacionog sistema (1997.) konkretizovan u dokumentu Realizacija plana dugoročnog razvoja informacionog sistema (1998.) omogućio je preduslove za stvaranje informatičke podrške obrazovnim procesima i poslovima upravljanja tim procesima. U tom smislu obezbeđena je tehnologija za:

- kompjutersku obradu podataka i računarsko komuniciranje
- savremeno administriranje i
- racionalno odlučivanje.

Konstituisana je i nova organizaciona jedinica (2000.g.) sa misijom uvođenja savremene edukacije, savremenog informisanja, komuniciranja i odlučivanja i uvođenja sistema kvaliteta u nastavnu delatnost Škole (sada KPA) - Kibernetiski edukacioni i razvojni centar (KERC). Projektovan je i implementiran Informacioni sistem sa više podistema koji obezbeđuju potrebne preduslove za modernizaciju obrazovnog procesa i poslovanja. Informacioni sistem KPA obuhvata:

- *Podsistem Savremena edukacija*
 - Produkcija prezentacionih materijala (izrada, izmena i arhiviranje raznih multimedijjskih sadržaja)
 - Produkcija udžbeničke literature (izrada elektronskih udžbenika, priručnika i praktikuma)
 - Produkcija edukacionih materijala
 - Tehnologija e-učenja firme IBM Lotus (LearningSpace – Virtual Classroom)
 - E-platforma i e-sadržaji
- *Podsistem Nastava*
 - Nastavnici i saradnici
 - Materijalno obezbeđenje nastave
 - Planiranje nastave
 - Realizacija nastave
- *Podsistem Elektronska dokumentacija*
 - Dokumentacioni fond InDok sistema
 - Aplikacije InDok sistema
 - Zaštita InDok sistema
- *Podsistem Moderno kancelarijsko poslovanje*
 - Programski sistem obrada teksta
 - Programski sistem planer
- *Podsistem Informatička podrška odlučivanju(IPO)*
 - Statistički modeli
 - Modeli ekspertize

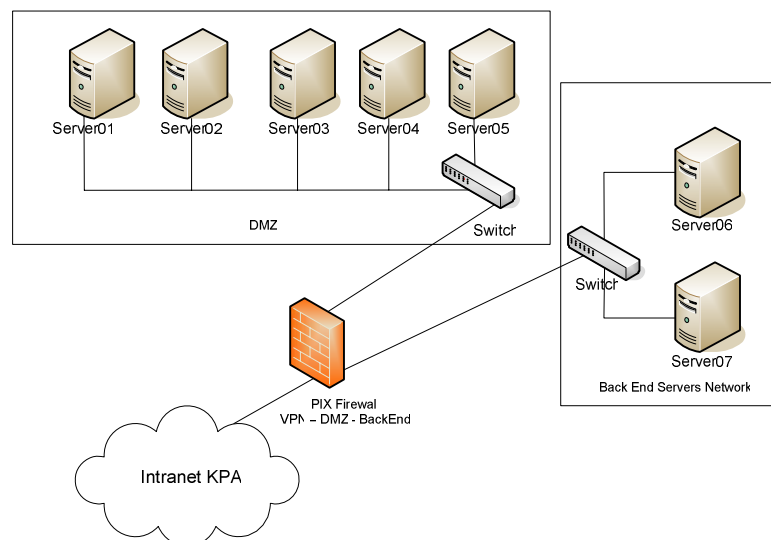
- Modeli poslovnog komuniciranja
- Aplikacije Sistema IPO

3.2. Zaštita Informacionog sistema KPA

Bezbednost pristupa i korišćenja Informacionog sistema KPA obezbeđena je implementacijom Domino modela zaštite. Primenjene su preporuke i mehanizmi zaštite navedeni pod 2.1, 2.2, 2.3, 2.5 i 2.6 u ovom radu.

U Kriminalističko policijskoj akademiji(KPA) ostvarena je propisana fizička zaštita. Serveri su fizički smešteni u klimatizovanu zasebnu prostoriju (serverska sala). Pristup serverskoj sali je jasno definisan i ograničen na ovlašćena lica od strane uprave KPA. Prostorija je pod stalnim video nadzorom i bezbednosnim alarmnim sistemom, kao i savremenim protivpožarnim sistemom.

Na serverima KPA instaliran je Windows 2000 Advanced Server operativni sistem. Glavni administrator sistema je odgovoran za primenu metodologije zaštite na nivou operativnog sistema. Izvršena su sva preporučena podešavanja od strane Microsofita radi povećanog nivoa bezbednosti. Na nivou celokupnog intraneta instaliran je korporativni antivirus, kao i WSUS, sistem za automatski update u okviru LAN mreže svih servera i klijenata.



Slika 3. Fizička šema arhitekture IS KPA [1]

Sistem zaštite IS KPA na mrežnom nivou realizuje se kroz tri zone. Prva zona na slici 3 predstavlja Intranet mrežu KPA. Ova zona je sastavljena od LAN (klijenti KPA Zemun) i WAN korisnika (Naučno-istraživački centar na Avali i Intranet-a MUP-a). Štiti se virtuelnim privatnim mrežama(VPN). VPN su realizovane primenom mehanizma VPN Gateway na udaljenim lokacijama i štite saobraćaj od svih radnih stanica unutar udaljene lokacije primenom IPSec protokola. Na obe strane VPN kanala nalaze se Cisco PIX Firewall uređaji, koji imaju i funkciju VPN Gateway-a. Granicu između ove zone i demilitarizovane zone (DMZ) čini firewall uređaj, a takođe i granicu između DMZ i mreže pozadinskih servera (Back-end Network). Celokupan saobraćaj iz dela mreže nižeg nivoa zaštite je zabranjen u deo pod višim nivom zaštite. [1]

Na prvom Domino serveru kreirani su svi korisnici Informacionog sistema KPA, tj njihovi ID-jevi. ID svakog korisnika je zaštićen i pravo pristupa je dodeljeno samo pripadajućem ID-u. ID jedinstveno identifikuje svakog korisnika ponaosob i daje mu prava pristupa serveru.

Zaštita Lotus notes aplikacija obezbeđena je konfigurisanjem kontrolnih pristupnih listi (ACL). Za svaku pojedinačnu aplikaciju konfigurisana je ACL sa tačno određenim pravima pristupa korisnika kao i njihovih uloga, koje određuju dozvoljeni nivo izmene date aplikacije.

ZAKLJUČAK

Informacioni sistem KPA zasnovan je na okruženju Lotus Domino (IBM) koje sadrži savremene mehanizme zaštite usmerene ka smanjenju rizika koji unosi dominantna bezbednosna pretnja - ljudski faktor. Iskustvo u korišćenju i održavanju sistema potvrđuje da najznačajnije probleme koji rezultuju u otkazu usluge sistema, stvaraju nestručni i nemarni korisnici.

Primenjeni model zaštite, kao i okruženje kome pripada, sadrži mogućnosti izmene i daljeg razvoja (fleksibilnost i skalabilnost) u skladu sa savremenim trendovima modernog poslovanja (elektronska komunikacija, sistemi poruka i upravljanje dokumentima) i edukacije (e-learning). Ovo je veoma značajno za novu instituciju, kakva je Kriminalističko-policijska akademija. U svom budućem radu ovakvoj instituciji je neophodan dalji razvoj postojećeg sistema za upravljanje i koordinaciju elektronskim poslovanjem, realizovan na postojećem intranetu. Zajedno sa novim mogućnostima i prednostima modernog poslovanja, stižu i novi izazovi u vidu novih bezbednosnih pretnji. Zaštita informacionog sistema je od vitalnog značaja, za njegovo funkcionisanje, a samim tim i za održivost poslovnog sistema. Posledice narušavanja bezbednosti kao što su:

- gubitak operativnog vremena usled pada sistema,
- oštećenje mrežne (HW i SW) infrastrukture,
- gubitak poslovnog kredibiliteta,
- neprimetna krađa ili fino oštećenje podataka (data diddlers),
- obmana korisnika da je sve u redu,
- otkaz usluge sistema (denial of service) itd.

predstavljaju dovoljno ozbiljne pretnje, tako da zaštita bezbednosti predstavlja primarnu poslovnu odluku i omogućava minimizaciju poslovnog rizika.

LITERATURA

1. KPA Sistemska arhitektura
2. Randall Tamura, Lotus Notes and Domino Server, Unleashed, Second Edition
3. Andrew Dahl, Lotus Notes: Administrator's Survival Guide
4. Intranets Unleashed, Dwayne Gifford
5. Lotus Notes Administrator's Guide, Bret Swedee
6. W. Tworek i dr (2004.) Lotus Security Handbook