Fakultet inženjerskih nauka Univerziteta u Kragujevcu

Nikola S Novaković

Zaštita Baze Podataka

master rad

Kragujevac, 2013.

Fakultet inženjerskih nauka Univerziteta u Kragujevcu

Naziv studijskog programa : Master Industijsko Inženjerstvo
Nivo studije : Master akademske studije
Modul : Poslovno informacioni sistemi
Predmet : Projektovanje informacionih sistema i baze podataka
Br. Indeksa: 612/2012

Nikola S Novaković

Zaštita Baze Podataka

Master rad

Komisija za pregled i odbranu :

1. **Dr Milan Erić - Mentor**
2. **_____**
3. **_____**

Datum odbrane : _____
Ocena : _____

U okviru ovog master rada kandidat treba da :

Prouči i na konkretnom primeru prezentira bezbednost odnosno zaštitu baza podataka. Rad treba da obuhvati uvodna razmatranja vezana za osnovne postavke etičke i pravne zaštite baza podataka, prikaz glavnih pretnji zaštiti informacija, opis različitih mehanizama odbrane koji se koriste za zaštitu, prednosti i nedostatke istih, kao i načine primene. Na konkretnom sistemu za upravljanje bazom podataka prikazata primenu zaštite.

Preporučena literatura

[1] Lazarević B : **Baze podataka** , FON Beograd , Beograd 2003 .
[2] Pavlović - Lažetić G:.**Osnove relacionih baza podataka**, Matematički fakultet, Beograd, 2000.
[3] Poliščuk J:. **Projektovanje informacionih sistema**, Elektrotehnički fakultet, Podgorica, 2007.
[4] Rajner K., Turban E.: **Uvod u informacione sisteme**, John Vilei & Sons, Inc, 2009.

Kragujevac, mentor:

Milan Erić Dr

_____

Izjavljujem da sam ovaj master rad uradio samostalno, služeći se stečenim znanjem i iskustvom kao i navedenom literaturom.

Broj indeksa Ime i prezime

612/2012 Nikola Novaković

Rezime rada :

U ovom radu je prikazana zaštita podataka, baze podataka na osnovu, zakona koji se koriste na području Srbije, ISO standard za zaštitu informacija, osnovnih deset pretnji koji se javljaju i rešenja za njihovo otklanjanje. Opisana je zaštita pomoću kriptograifije i na kraju primer koji omogućava zaštitu baze u Access-u na osnovu Security Wizarda kojim je korak po korak objašnjeno kako se štiti baza tako da kada bi se njoj pristupilo potreban je Login.

Ključne reči : Baza podataka, Zaštita, Sigurnost, Šifrovanje

Abstract :

In this paper, a data protection, database on the basis of laws which are used in Serbia, the ISO standard for information security, the ten main threats that arise as solutions for their elimination. Described by Cryptography protection and at the end of such arrangements to protect database in Access from Security Wizard which is a step by step explains how to protect the database so that if it approached Login required.

Keywords : Database, Protecion, Security, Cryptography

Sadržaj:

1. Uvod

Kompjuteri i tehnologije su postali sastavni deo društva, a njihova svakodnevna upotreba se ne dovodi u pitanje. U modernim državama, celokupna infrastruktura je automatizovana do određenog stepena, čineći da se svakodnevne životne aktivnosti odvijaju brže i lakše. Upravo se u takvom načinu života krije i najveća ranjivost. Prestanak protoka informacija na kritičnoj infrastrukturi, bilo da je reč o prirodnoj katastrofi ili o napadu koji je proizveo pojedinac ili grupa, može državu da dovede do kamenog doba. Upravo zbog toga se u doktrinarnim dokumentima, vodećih vojnih i ekonomskih sila, akcenat stavlja na zaštitu najvažnijih infrastrukturnih segmenata, a posebno sledećih:

– Informacija i komunikacija
– Bankarstva i finansija
– Energije, ukljucujući električnu energiju, naftu i gas i
– Transportnog sistema.

Ovde je važno uočiti redosled kojim su nabrojani infrastrukturni segmenti. Informacije i komunikacije imaju vrhunski prioritet. Isto tako kao što država štiti informatičku infrastrukturu, tako i privatne kompanije stavljaju akcenat na zaštitu informacija. Savremeno poslovanje je nezamislivo bez komunikacija i baza podataka. Baze podataka predstavljaju izvor informacija za većinu aplikacija koje pomažu u obavljanju primarnih aktivnosti svakog poslovanja. Širenjem tržišta, a samim tim i razvojem organizacija, bez obzira da li su one državne ili privatne, uočena je primena sistema baza podataka kao ključne tehnologije za upravljanje podacima i pomoćnog sredstva za donošenje odluka.[1]

Nakon kratkog uvoda u drugom delu rada priakzani su zakonom koji postoje u Srbiji i koji se primenjuju i novi zakoni koji će se primenjivati pošto težimo evro – atlanskim integracija. Takođe u drugom delu rada je opisan ISO standardom 27001 i 27005 koji se odnosi na zaštitu informacija i njenu bezbednost, ovaj standard se bave uslugama u oblastima koje su na bilo koji način povezane sa Informacionim tehnologijama i potrebom za očuvanje poverljivosti informacija, zatim je opisana intelektuala svojina koja omogućava zaštitu patenata, muzičkih i video i drugih sadržaja i nakon ovoga sledi opis deset najčešćih pretnji na bazu koji se javljaju i rešenja za njeno otklanjanje.

U Trećem delu rada prikazana su karkteristike ključeva jer bezbednost kriptosistema zavisi od bezbednosti i pažljivog rukovanja ovim ključevima, razmatranje obuhvata naglasak na to da bilo koji dati ključ treba koristiti u jednu jedinu svrhu, te da familije ključeva podržavaju taj koncept.

Nakon ovh zakona, standarda, realnih pretnji koji se javljaju i metoda zaštite ključa u sledećem delu rada urađen je primer, koji je urađen u Access-u gde je opisan istorijat, zatim dva realna primera koja se koriste u zaštiti baze i njenog sadržaja.

2. Pravna zastita baze podataka u srpskom pravu

Baza podataka je kolekcija podataka organizovanih za brzo pretraživanje i pristup, koja zajedno sa sistemom za administraciju, organizovanje i memorisanje tih podataka, čini sistem baze podataka. Iz ugla korisnika, podaci su na neki logički način povezani. Oni predstavljaju neke aspekte realnog sveta.[1]

Zaštita podataka - proces kojim se osiguravaju podaci od oštećenja pri prenosu i kontrola pristupa podacima u računaru. Na taj način zaštita podataka osigurava privatnost, Koristi se za zaštitu, kako privatnih, tako i javnih podataka. Zaštita podataka se koristi pri prenosu podataka osetljivog sadržaja (vladinih dokumenata, bankovnih podataka, dokumenata državnih služba, podataka velikih poduzeća...). Kako bi podaci na svoje odredište stigli netaknuti i u istom obliku u kojem su poslani, podatke zaštićujemo od oštećenja u prenosu i neovlašćenih upada ili preusmjeravanja tokom prenosa. Takođe je potrebno zaštiti i podatke koji su u našem računaru – od neovlašćenih upada sa istog ili drugih računara i od napada virusa.

U Srbiji postoji relativno mali broj zakona i propisa koji definišu informacione sisteme. Kada su u pitanju baze podataka, prvi zakon koji je obuhvatio njihovu zaštitu objavljen je 1998. godine, gde su prvi put definisana i prava proizvođača baze podataka kao predmet zaštite srodnih prava (zasnovan na Direktivi 96/9/EC Evropskog parlamenta iz 1996.godine o pravnoj zaštiti baze podataka). 2009. godine u okviru Zakon o autorskom i srodnim pravima regulisane su posebne odredbe koje se odnose na baze podataka. Osim pravne, postoje i tehničke mere zaštite baze podataka.

1) Pojam Baze podataka i Autorska prava

Baza podataka se definiše kao strukturirana kolekcija podataka koja postoji relativno dugo, koju koristi i održava više korisnika odnosno programa i koja se koristi za skladištenje informacija. Razmatrajući ovu definiciju, postavlja se pitanje da li je baza podataka autorsko delo? Da bi se neka zbirka ili kolekcija podataka proglasila autorskim delom ili zaštitila autorskim pravom mora se utvrditi njena originalnost, bez obzira ukoliko njeni elementi nisu zaštićeni autorskim pravom. Baza podataka se sastoji iz delova tj. logično prikupljenih celina koje su na sistematičan način povezane i grupisane u određene katagorije u koje je uložen intelektualni napor, kreativnost i lični doprinos i koje su dostupne elektronskim ili nekm drugim putem. Ove karakteristike su osobine autorskog dela, pa i zaslužuju da budu zaštićene kao intelektualna svojina. Bitno je napomenuti da Zakon o autorskom i srodnim pravima pod bazom podataka ne podrazumeva računarski program koji se koristio za njeno stvaranje ili rad (član 138 stav 2).[2]

2) Proizvodjač Baze podataka

Pod proizvođačem baze podataka se smatra fizičko ili pravno lice koje je sačinilo bazu podataka, uložilo napor u sakupljanje, proveru ili prezentaciju njenog sadržaja i podataka (član 137.). Svaki proizvođač baze podataka ima imovinska prava tako da drugima može da zabrani ili dozvoli umnožavanje, zakup ili javno saopštavanje kako cele baze podataka tako i nekih njenih delova, prema članu 140 Zakona. o autorskom i srodnim pravima. Sva prava proizvođača traju 15 godina od nastanka baze podataka. Ukoliko dođe do dodavanja novih sadržaja u bazu

podataka, brisanja nepotrebih ili promene pojedinih delova ili cele baze dobija se nova verzija baze podataka. Svaka nova verzija donosi proizvođaču dodatnih 15 godina prava na korišćenje (član 147 stav 2 i 3). Ukoliko je baza podataka objavljena javnosti, rok od 15 godina zadržavanja prava važi od momenta kada je objavljena, a ne od momenta kada je sačinjena.

3) Ograničenja proizvođača baze podataka

Zakon o autorskom i srodnim pravima Republike Srbije ne sadrži specifična ograničenja prava proizvođača baze podataka, mada i sam proizvođač može prekršiti određene zakonske odredbe ukoliko se ne navede izvor iz koga su delovi baze podataka preuzeti.

4) Pravna zaštita proizvođača baze podataka

Objavljivanje sadržaja baze podataka ili nekih njenih delova, od strane korisnika, moguće je samo u slučaju posedovanja odgovarajuće licence ili saglasnosti nosioca prava. U ugovoru o ustupanju prava na korišćenje baze podataka jasno su definisana prava i obaveze nosioca prava i korisnika baze podataka:

a) Nosilac prava korisniku predaje bazu podataka i potrebnu dokumentaciju koja sadrži upustva za unos, korišćenje i pretragu podataka.

b) Korisnik može da napravi kopije baze podataka samo po ugovoru i po dogovorenom broju.

c) Nosilac prava je dužan da zameni bazu podataka u slučaju oštećenja, samo ako korisnik nije odgovoran za oštećenje.

U praksi se često dešava da se pojedini delovi baze podataka objavljuju na internetu, u komercijalne svrhe, radi reklamiranja, obavljanja određenih delatnosti, bez dozvole preradi, objavi ili na bilo koji način iskoristi tuđa baza i sl. Ako su prava proizvođača baze podataka povređena, proizvođač baze podataka ima sva zakonska ovlašćenja da pismenim putem zatraži od korisnika da ne koristi preuzete materijale ili da podnese krivičnu prijavu. U Zakonu o autorskom i srodnim pravima Republike Srbije predviđene su sankcije za privredni prestup zbog povrede prava proizvođača baze podataka i novčane kazne (za pravna lica od 100 000 do 3000 000 Dinara; Za preduzetnike od 50.000 do 500.000 dinara (član 215 I 216)).[3]

2.1 ISO 27001 i 27005 – Sistem upravljanja informacionom sigurnošću

ISO 27001 je međunarodni standard koji se odnosi na zaštitu i bezbednost informacija**.** Standard podleže različitim područjima primene kao i za razlikovanje mogućih procesa u organizaciji koji su povezani sa upravljanjem kontrole sigurnosti kao što su: politika sigurnosti, sigurnost organizacije, kontrola i klasifikacija izvora, sigurnost osoblja, sigurnost materijalnih dobara i životne sredine, operativno upravljanje i komunikacija, kontrola pristupa, razvoj i održavanje raznih sistema i upravljanje kontinuitetom poslovanje.

Ova serija obuhvata standarde koji: definišu zahteve za ISMS (information security management system) kao i zahteve za tela koja sertifikuju ISMS; obezbeđuju podršku, detaljna uputstva i instrukcije za celokupan proces planiraj-uradi-proveri-deluj (Plan-Do-Check-Act); daje specifična sektorska uputstva za ISMS i ocenjivanje usaglašenosti za ISMS.[4]

Standard ISO 27001 je značajan standard za organizacije koje se bave uslugama u oblastima koje su na bilo koji način povezane sa Informacionim tehnologijama i potrebom za očuvanje poverljivosti informacija. Njegova implementacija i primena omogućavaju bolju saradnju sa sličnim organizacijama širom sveta koje posluju po ovom modelu. Ovim standardom, organizacije demonstriraju svojim korisnicima i ostalim zainteresovanim stranama da posluju sa poslovnim procesima na bazi principa sigurnosti i da je poslovna politika usmerena na stalna poboljšavanja u sistemu menadžmenta za bezbednost informacija i procesima pružanja usluga povezanim sa njim.

Implementacija sistema zaštite i bezbedosti informacija pruža uverenje klijentima i poslovnim partnerima da se prema informacijama postupa odgovorno i da se one koriste i distribuiraju profesionalno i sigurno.

Prednosti ISO 27001 :

- konkurentska prednost,
- smanjenje rizika od oštećenja i gubitka informacija, a samim tim i troškova,
- usaglašenost sa važećim zakonskim propisima,
- veće poverenje klijenata, zaposlenih, saradnika, institucija i svih zainteresovanih strana zbog znanja da su njihovi podaci bezbedni,
- postojanje odgovornosti za bezbednost informacija od strane svih i na svim nivoima u organizaciji.

1) Istorijat standarda informacione sigurnosti

Slika 1. Istorijat

Serija ISO 27000 :

- ISO 27000 – Rečnik termina koji se koriste u „ISO 27000“ seriji standarda;
- ISO 27001:2005 – Sistem upravljanja informacionom sigurnošću;
- ISO 27002:2007 – Kodeks postupaka za upravljanje informacionom sigurnošću;
- ISO 27003 – Vodič za implementaciju sistema za upravljanje informacionom sigurnošću;
- ISO 27004 – Merenje i metrike efikasnosti sistema informacione sigurnosti ;
- ISO 27005 – Standard za upravljanje rizicima informacione sigurnosti;
- ISO 27006:2007– Zahtevi za postupkom analize i sertifikovanja standarda;
- ISO 27007 – Uputstva za analizu sistema za upravljanje informacionom sigurnošću;
- ISO 27011 – Uputstva za uspostavljanje sistema za upravljanje informacionom sigurnošću u telekomunikacionom sektoru;
- ISO 27031 – Specifikacije za IKT (informaciono komunikacione tehnologije) odsek pripremljenosti poslovne neprekidnosti rada (Business Continuity Planning, skr. BCP);
- ISO 27032 – Uputstva za Cyber – sigurnost (Internet sigurnost u slobodnom prevodu);
- ISO 27033 – Uputstva za mrežnu sigurnost;
- ISO 27034 – Uputstva za sigurnost aplikacija;
- ISO 27799 – Sigurnosni sistemi u zdravstvu.

Koristi od standardizovanog načina pristupa informacionoj sigurnosti :

1) Povećana pouzdanost i sigurnost sistema
2) Povećanje profita
3) Smanjenje troškova
4) Pravna usklađenost
5) Poboljšano upravljanje
6) Poboljšani odnosi sa klijentima i partnerima

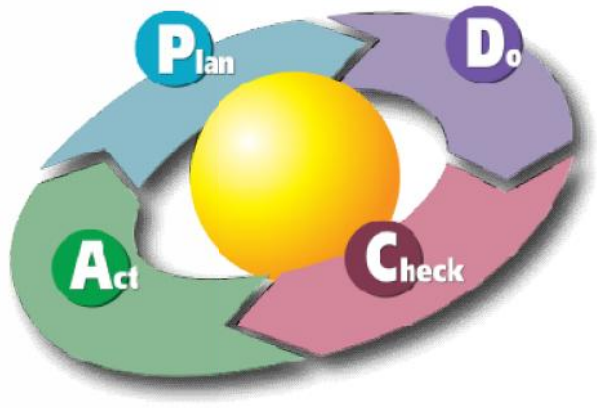
ISO/IEC 27001 standard :

1. Standard ISO/IEC 27001 opisuje proces uvođenja sistema za upravljanje sigurnošću informacija (Information Security Management System - ISMS)
2. Cilj procesa je postići sigurnost informacija u tri glavna aspekta:
    a. Poverljivost,
    b. integritet i
    c. raspoloživost,
3. Uzimajući pritom u obzir i relevantne resurse, politike, procedure i informacione sisteme

Sadržaj ISO 27001

Sistem upravljanja sigurnošću informacija:
1. Opšti zahtevi
2. Utvrđivanje i upravljanje ISMS-om
3. Zahtevi vezani za dokumentaciju
4. Odgovornost rukovodstva
5. Obaveze rukovodstva
6. Upravljanje resursima
7. Interne provere ISMS
8. Preispitivanje ISMS od strane rukovodstva
9. Poboljšavanje ISMS-a

PDCA model primenjen na sisteme za upravljanje sigurnošću informacija



Slika 2. PDCA model

PLAN

Podrška rukovodstva

Definisanje opsega sistema za upravljanje sigurnošću informacija

Kreiranje politike ISMS

Utvrđivanje pristupa ocene rizika

Identifikacija, analiza i procena rizika

Identifikacija i procena opcija za obradu rizika

Odabir sigurnosnih kontrola

Odobrenja i ovlašćenja rukovodstva

Kreiranje izjave o primenjivosti

DO

Izrada i implementacija plana za upravljanje sigurnosnim rizicima

Implementacija sigurnosnih kontrola i definisanje kako će se meriti efikasnost kontrola

Sprovođenje obuke i razvoj svesti

Upravljanje operacijama i resursima

Uočavanje i reagovanje na sigurnosne incidente

CHECK

Izvršavanje procedura za nadzor sistema

Provera efektivnosti kontrola i sistema

Provera nivoa rizika i rezidualnog rizika

Interne provere

Preispitivanje od strane rukovodstva

Ažuriranje planova i beleženje aktivnosti

ACT

Implementacija metoda za poboljšanje sistema

Definisanje i realizacija korektivnih i preventivnih mera

Interno informisanje o efektivnosti sistema

Potrebna dokumenta :

1. Izjava o sigurnosnoj politici i njenim ciljevima;
2. Opseg važenja („Scope“) sistema za upravljanje sigurnošću informacija;
3. Procedure i kontrole na koje se sistem za upravljanje sigurnošću informacija oslanja;
4. Opis metodologije za procenu rizika;
5. Izveštaj o proceni rizika;
6. Plan obrade rizika;
7. Procedure potrebne za planiranje, održavanje i kontolisanje sigurnosnih procesa;
8. Izjava o primenljivosti.

Definisanje politike

Sigurnosna politika treba da:

1. sadrži odnos organizacije ka pojmu informacione sigurnosti;
2. pruži okvir za postavljanje ciljeva, kao i da uspostavi smernice i principe za sve akcije;
3. uzme u obzir sve poslovne, zakonske i ugovorene sigurnosne zahteve;
4. bude usklađena sa strategijom upravljanja rizicima;
5. utemelji kriterijume za evaluaciju rizika;
6. bude odobrena od strane rukovodstva organizacije

Definisanje opsega

U samom standardu su navedene određene smernice koje se koriste za definisanje opsega važenja sistema:

a. Preporučuje se izrada grafičkog prikaza ili dijagrama same strukture organizacije, kako bi se lakše sagledale sve specifičnosti organizacije;
b. Neophodno je izraditi dokument sa opisom opsega važenja, koji je usklađen sa organizacionom strukturom;
c. Preporučuje se izrada dokumenta u kome će biti popisana celokupna oprema i resursi koji će biti obuhvaćeni ovim sistemom;
d. Takođe se preporučuje izrada grafičkog prikaza lokacija ove opreme

Izjava o primenjivosti

Izjava o primenljivosti (engl. Statement of Applicability“, „**SoA**“) treba da sadrži sledeće elemente:

a) Kontrolne ciljeve, kontrole i razlog njihovog odabira,
b) Kontrolne ciljeve i kontrole koje su već implementirane,
c) Sve kontrolne ciljeve i kontrole koje su isključene, kao i razlog njihovog isključenja

Upravljanje rizikom kroz obradu rizika i donošenje odluka :

a) Donošenje odluka
b) Umanjivanje rizika
c) Svesno i objektivno prihvatanje rizika
d) Prenošenje rizika
e) Rezidualni rizik

Obezbeđivanje resursa

Organizacija mora obezbediti resurse potrebne da se:

a) utvrdi, primeni, sprovodi, nadgleda poboljšanje ISMS
b) obezbedi da procedure podržavaju zahteve posla
c) Identifikuju pravni zahtevi i ugovorne obaveze vezane za sigurnost
d) održi sigurnost primenom svih utvrđenih kontrola
e) objave rezultati nadzora i reaguje na rezultate
f) poboljša efikasnost ISMS-a

Ulazni podaci u preispitivanje od strane rukovodstva

a) Rezultati provera i nadzora
b) Povratne informacije od zainteresovanih strana
c) Primenjive tehnike, proizvodi ili procedure za poboljšanje učinka i efikasnosti ISMS
d) Status preventivnih i korektivnih mera
e) Slaba mesta ili pretnje koje nisu rešavane na adekvatan način pri prethodnoj proceni rizika
f) Rezultati merenja efikasnosti
g) Status mera definisanim na prethodnim preispitivanjima
h) Promene koje mogu da utiču na ISMS
i) Preporuke za poboljšanje

Politika sigurnosti

1. Organizacija informacione sigurnosti

1.1 Interna organizacija
1.2 Spoljni učesnici

2. Upravljanje imovinom

2.1 Odgovornost za imovinu
2.2 Klasifikacija informacija

3. Sigurnost ljudskih resursa

3.1 Pre stupanja u radni odnos
3.2 Za vreme radnog odnosa
3.3 Prestanak ili promena radnog odnosa

4. Fizička sigurnost i sigurnost vezana za okruženje

4.1 Sigurna područja
4.2 Sigurnosna oprema

5. Upravljanje komunikacijama i radom

5.1 Operativne procedure i odgovornosti
5.2 Upravljanje pružanjem usluga trećih lica
5.3 Planiranje i prijem sistema
5.4 Zaštita od zlonamernog i mobilnog koda
5.5 Podrška (Back-up)
5.6 Upravljanje sigurnosnom mrežom
5.7 Rukovanje medijima
5.8 Razmena informacija
5.9 Usluge elektronske trgovine
5.10 Nadzor

6. Kontrola pristupa

6.1 Poslovni zahtevi kontrole pristupa
6.2 Upravljanje pristupom korisnika
6.3 Odgovornost korisnika
6.4 Kontrola pristupa mreži
6.5 Kontrola pristupa operativnim sistemima
6.6 Kontrola primene i pristupa informacijama
6.7 Bežični rad računara i rad na daljinu

7. Nabavka, razvoj i održavanje IS

7.1 Sigurnosni zahtevi IS
7.2 Korektna obrada u aplikacijama
7.3 Kriptografske kontrole
7.4 Sigurnost sistemskih fajlova
7.5 Sigurnost u razvojnim i pratećim procesima
7.6 Upravljanje tehnički slabim tačkama

8. Upravljanje incidentima

8.1 Izveštavanje o događajima i slabostima
8.2 Upravljanje incidentima

9. Upravljanje kontinuitetom posla

10. Poštovanje

10.1 Poštovanje pravnih zahteva
10.2 Poštovanje sigurnosne politike i standarda
10.3 Značaj provere informacionih sistema

Referenca	**Oblast**	**Kontrola**
A.11.4	Kontrola pristupa mreži	
A.11.4.1	Politika upotrebe mrežnih usluga	Korisnicima će biti omogućen pristup samo servisima za koje su dobili specijalno ovlašćenje za korišćenje
A.11.4.2	Potvrda korisnika za spoljne konekcije	Odgovarajuće metode potvrde će se koristiti da se kontroliše pristup od strane udaljenih korisnika
A.11.4.3	Identifikacija mrežne opreme	Automatska identifikacija opreme će biti sredstvo za potvrdu konekcija sa specifičnih lokacija i opreme
A.11.4.4	Zaštita dijagnostičkih i konfiguracijskih portova	Fizički i logički pristup dijagnostičkim i konfiguracijskim portovima biće kontrolisan
A.11.4.5	Segregacija u mrežama	Grupe informacionih servisa, korisnici i informacioni sistemi biće zaštićeni na mreži
A.11.4.6	Kontrola mrežnog povezivanja	Za zajedničke mreže mogućnost konekcije će biti ograničena, u skladu sa politikom kontrole pristupa i zahtevima aplikacija

Tabela 1 Oblast i kontrola

2.1.1 ISO 27005

Prvenstvena namena standarda „ISO/IEC 27005“ je da pruži smernice za upravljanje rizikom prilikom uspostavljanja sistema za upravljanje sigurnošću informacija, odnosno da pruži dodatne smernice prilikom implementacije „ ISO/IEC 27001 “.

a) Deo za procenu rizika informacione sigurnosti (Information Security Risk Assessment - ISRA);
b) Deo za tretiranje rizika (Information Security Risk Treatment);
c) Deo za prihvatanje rizika (Information Security Risk Acceptance);
d) Deo za komunikaciju u vezi nastalih rizika (Information Security Risk Communication);
e) Deo za nadzor i preispitivanje u vezi nastalih rizika (Information Security Risk Monitoring and Review)

Procena rizika

Prema preporukama standarda ISO / IEC 27005 procena sigurnosnog rizika uključuje analizu i evaluaciju rizika. Analiza rizika uključuje:

a) Identifikaciju resursa;
b) Identifikaciju zakonskih i poslovnih zahteva ;
c) Procenu vrednosti identifikovanih resursa, uzimajući u obzir zakonske i poslovne zahteve i posledice u slučaju gubitka poverljivosti;
d) Identifikaciju pretnji i ranjivosti resursa; i
e) Procenu verovatnoće pojave pretnji i ranjivosti.

Faza evaluacije rizika uključuje:

a) Izračunavanje rizika i
b) Evaluaciju rizika u odnosu na predefinisanu skalu rizika.

1) Identifikacija resursa

Kategorija	Opis
Informacije	Informacije predstavljaju najvažniji tip resursa koji je potrebno zaštititi, bez obzira u kom obliku se one nalaze (npr. baze podataka, datoteke sa podacima, sistemska dokumentacija, ugovori, priručnici, smernice, planovi obezbeđenja kontinuiteta poslovanja, obrazovni materijali i sl.)
Procesi i usluge	Procesi i usluge uključuju poslovne procese, aplikacione aktivnosti, operativne usluge, komunikacijske usluge i ostale usluge koje omogućavaju procesiranje informacija, npr. grejanje, rasveta, struja i sl.
Softver	Uključuje aplikativni softver, sistemski softver, razvojne alate, pomoćne aplikacije i sl.
Hardver	Uključuje računare, komunikacionu opremu, razne vrste medija (papire, CD i DVD diskove .... i sl.), tehničku opremu (izvore napona, klimatizaciju) i sl.
Ljudi	U ovu kategoriju spada osoblje, klijenti, korisnici usluga i svi ostali koji imaju bilo kakvu ulogu u procesu unosa i/ili procesiranja informacija.

Tabela 2 Indetifikacija resursa

2) Identifikacija zakonskih i poslovnih zahteva

Sigurnosni zahtevi svake organizacije dolaze iz tri glavna izvora:

a) Pretnje i ranjivosti, koje mogu rezultovati velikim gubicima u slučaju realizacije;
b) Zakonski i ugovorni zahtevi,
c) Svi principi, ciljevi i zahtevi organizacije na koje se oslanjaju poslovni procesi, a koji se odnose na informacione sisteme organizacije

3) Procena vrednosti resursa

a) Jedan od načina izražavanja vrednosti resursa je da se u obzir uzmu posledice incidenata po poslovni proces, npr. modifikacije, uništenja ili gubitka raspoloživosti informacija. Ovakvi incidenti mogu dovesti do novčanih gubitaka ili do gubitka ugleda same organizacije.

b) Informacije o vrednosti resursa najbolje mogu dati sami vlasnici resursa. Kako bi se adekvatno procenila vrednost nekog resursa, potrebno je definisati skalu vrednosti resursa.

4) Identifikacija pretnji i ranjivosti sistema

Kada se vrši identifikacija ranjivosti sistema treba u obzir uzeti i slabosti resursa koje potiču iz:

a) Fizičkog okruženja samog resursa,
b) Administrativnih procedura i kontrola, uprave i osoblja koji njima raspolažu,
c) Poslovnih operacija,
d) Računarske i komunikacione opreme

5) Vrednovanje pretnji i ranjivosti sistema

a) Prilikom procene verovatnoće pojave pretnji, standard ISO / IEC 27005 propisuje da u obzir treba uzeti:
b) Namerne pretnje. Verovatnoća zavisi od znanja, motivacije i resursa kojima napadač raspolaže;
c) Slučajne pretnje. Verovatnoća se procenjuje pomoću statistike i na bazi ličnog iskustva;
d) Prethodne incidente;
e) Trendove. Pratiti raznu stručnu literaturu i izveštaje, koji mogu pomoći proceni situacije.

Verovatnoća pretnje	**Opis**
Mala verovatnoća (engl. „Low Likelihood“)	**Nije verovatno da će se pretnja pojaviti, tj. nije bilo nikakvih prethodnih incidenata, a statistike pokazuju da se pretnja neće pojaviti, jer za pretnju nedostaje motivacija**
Srednja verovatnoća (engl. „Medium Likelihood“)	**Postoji verovatnoća da će se pojaviti pretnja. Bilo je incidenata u prošlosti, a istraživanja pokazuju da postoje razlozi koji motivišu potencijalnog napadača.**
Visoka verovatnoća (engl. „High Likelihood“)	**Očekuje se pojava pretnje. Motivacija napadača je snažna, incidenti su u prošlosti bili učestali, a statistike potvrđuju veliku verovatnoću pojave pretnje.**

Verovatnoća ataka na ranjivost	**Opis**
Malo verovatno (engl. „**Unlikely**“)	Mala je verovatnoća da će se ranjivost eksploatisati. Postojeća zaštita je adekvatna.
Moguće (engl. „**Possible**“)	Moguća je eksploatacija ranjivosti, ali postoji zaštita.

Jako verovatno (engl. „**Highly Rrobable**“)	Lako je eksploatisati ranjivost, jer ili ne postoji nikakva zaštita ili postoji neadekvatna zaštita

Tabela 3 Vrednovanje pretnji

6) Izračunavanje i evaluacija rizika

a) Rizik se izračunava kao odnos vrednosti resursa, koja izražava posledice gubitka poverljivosti, integriteta i raspoloživosti informacija i verovatnoće pojave pretnji povezanih sa odgovarajućim ranjivostima.
b) Organizacija mora odabrati metodu za procenu rizika koja je najprikladnija njenim poslovnim procesima i sigurnosnim zahtevima.
c) Rizik se sastoji od dva faktora:
    - Posledice iskorišćavanja ranjivosti i
    - Verovatnoće pojave pretnje, odnosno iskorišćavanja ranjivosti.

2.2 Intelektualna svojina

Intelektualna svojina, poznatija kao IP (Intellectual Property), omogućava ljudima da poseduju svoju ispoljenu kreativnost i inovacije na isti način kao što je omogućeno da se poseduju materijalna dobra (Daniel M German,). Vlasnik intelektualne svojine može da kontroliše njenu upotrebu i za nju da bude nagrađen, što ohrabruje kreativnost kod ljudi od koje svi možemo da imamo velike koristi. U nekim slučajevima intelektualna svojina, odmah podleže zaštiti, dok je u drugim neophodna dodatna elaboracija ideje. Često, neće biti moguće zaštititi je i steći prava nad intelektualnom svojinom (Intellectual Property Rights), osim ako nije prijavljena i odobrena. Neke vrste IP zaštite stupaju na snagu odmah, bez registracije, ako postoji bilo kakav dokaz da je intelektualna svojina kreirana.[5]

2.2.1 Osnovi intelektualne svojine

Četiri osnovne oblasti, koje se vezuju za intelektualnu svojinu su:

• Patenti (pojam vezan za izume) – novi ili poboljšani proizvodi ili procesi koji se mogu primeniti u industriji. Patent dozvoljava pronalazaču, da određeni vremenski period, odlučuje kome će dati odobrenje za proizvodnju, prodaju i upotrebu tog proizvoda. Da bi proizvod bio registrovan kao patent, mora da ispunjava specijalne uslove. Većina patenata je napravljena da bi se primenjivala na poznatoj tehnologiji. Dakle, češće teže evoluciji nego revoluciji. Tehnologija patenta ne mora da bude kompleksna. Prava patenata su teritorijalna, različita su od države do države, a i zavise od oblasti nauke u kojoj se mogu primeniti. Iako su retko gde prava dobro formulisana, patent može da bude od velike vrednosti za pronalazača, a neretko može da bude od koristi i drugima. Preko ostvarivanja prava na licencu, drugi mogu koristiti patent. Tako Da, može se naučiti dosta iz tehnologije tuđih patenata.

• Trgovačke marke (pojam vezan za identitet brendova) – koristi se za robu i usluge da bi se napravila razlika među različitim proizvođačima. Trgovačka marka može biti reč, dizajn ili kombinacija istih koju koristi proizvođač da bi svoj proizvod ili uslugu učinio prepoznatljivim. Iako postoji poseban pojam marka usluge, retko se koristi. Trgovačke marke su pravno zaštićene, ali se prvenstveno koriste da bi se izdvojio brand koji tradicionalno obećava visok kvalitet proizvoda ili usluge. Očekivaćemo da se automobili koji nosi marku Rolls Royce biti superiorniji u odnosu na onaj koji nosi oznaku Yugo. Može se upotrebiti bilo kakav simbol ili ime da bi se identifikovao proizvod.

• Dizajn (pojam vezan za izgled proizvoda) – primenjuje se na izgled celog ili dela proizvoda. Dizajn podrazumeva boje, font, teksturu materijala, konture i oblik proizvoda kao i njegovu ornamentaciju.

• Autorska prava (pojam vezan za zaštitu) – primenjuje se na sve (muziku, film, software, multimediju...). Autorska prava omogućuju stvaraocu ekonomsku zaštitu u smislu da samo on ima pravo da raspolaže svojim delom kad hoće i koliko hoće. Ostali moraju da dobiju odobrenje autora, što podrazmeva novčanu naknadu. U državama sa zdravom ekonomijom i pravosuđem, vlasnik autorskih prava može da tuži (i vrlo da ima materijalne koristi od toga), svakoga ko neovlašćeno koristi ili promoviše njegovo delo. Pored toga autorsko pravo omogućava i moralnu

satisfakciju da ime stvaraoca uvek bude uz proizvod. Međutim, autorska prava ne mogu zaštititi ideje, naslove ili imena. Ipak, intelektualna svojina je mnogo opširnija. Obuhvata i poslovne tajne, geografske indikacije, prava proizvođaća i tako dalje. Da bismo što bolje razumeli IP moramo se podrobnije pozabaviti pobrojanim oblastima kao i nekim drugim pojmovima. Treba imati u vidu da se na jednu kreaciju može primeniti više aspekata intelektualne svojine (Ljiljana Tatic i Rastko Ilic).

2.2.2 Autorska prava, patenti i poslovne tajne

Poslovne tajne se u mnogome razlikuju od patenata, trgovačkih marki i autorskih prava. Na isti pronalazak se ne može primeniti i pravilo patenta i poslovna tajna – i jedan i drugi pojam su ekskluzivni. Kada je patent jednom odobren, biva objavljen tako da ceo svet sazna za njega, tako da ništa u izdatom patentu, po definiciji, ne može da bude poslovna tajna. Od kada se podnese prijava kancelariji koja odobrava patente, do momenta kada ista odobri patent, mora da prođe period razmatranja koji podrazumeva određen vremenski period. U toku razmatranja proizvod podleže pravilu poslovne tajne i nikakve informacije vezane za njega neće biti dostupne javnosti. To se dešava jer uvek postoji mogućnost da patent neće biti odobren. Pronalazač može da odluči da ne želi patent i da će se osloniti na zakone vezane za poslovne tajne. Sve u svemu, u ovakvim situacijama izbor je ili, ili. S druge strane, materijal za koji su specifična autorska prava, posebno računarski softver, može i mora da bude zaštićen i autorskim pravima i poslovnim tajnama. U nekim zemljama je ovaj problem premošćen na sledeci način: Obezbeđene su posebne dozvole za ovakve dualne načine zaštite. Materijal koji ne podleže zakonima o autorskim pravima može biti zašticen zakonima o poslovnim tajnama, tako što će se umanjena količina informacija biti prijavljena kancelariji koja se bavi autorskim pravima. Na primer, ako bismo razvili program koji će na osnovu verovatnoće birati profitabilne akcije, sam program bismo zaštitili zakonima o autorskim pravima, a algoritam koji koristimo bi potpao pod poslovnu tajnu. Dakle, u takvim slučajevima kancelarije koje se bave autorskim pravima dozvoljavaju zaštitu koda i ne zahtevaju da se oda algoritam. Poslovne tajne i trgovačke marke su nasledno eksluzivni u odnosu jedan na drugog. Svrha trgovačke marke je da poboljša prepoznavanje proizvoda ili kompanije, nasuprot poslovnoj tajni kojoj je cilj da drži neke informacije što dalje od potrošača.

2.2.3 Softverska piraterija

Softverska piraterija je neovlašćeno kopiranje računarskog softvera. Iako većina korisnika danas shvata da je ovo pogrešno, mnogi se ne obaziru na to jer ne shvataju važnost činjenice da je taj isti softver vredna intelektualna svojina. Softverska piraterija je postala kontraverzno pitanje još kada je Internet prvi put stekao popularnost. Što se više povećavao broj korisnika, uporedo sa njim je neovlašceno kopiranje počelo da biva sve veći problem. Ovo se dešava zbog vrlo lakog pristupa već ukradenim delima i zbog neverovatno niske cene reprodukcije. Softverska piraterija se može podeliti u sledeće kategorije:

- Piraterija krajnjeg korisnika
- Klijent – Server Overuse
- Internet piraterija
- Hard – disk loading
- Softver counterfeiting

Krajnji korisnik je konačni korisnik računarskog sistema ili proizvoda. Piraterija krajnjeg korisnika se pojavljuje kada pojedinac ili kompanija, neovlašceno koriste ili reprodukuju softver. Ovo obuhvata, kako korišćenje jednog licencnog proizvoda pri instalaciji na više računara, kopiranje diska za dalju distribuciju, tako i upotrebu ograničenog, akademskog softvera u komercijalne svrhe. Danas, postoje hiljade piratskih sajtova na Internetu, na kojima se virtuelno nalazi svaki softverski proizvod koji se može naći u slobodnoj prodaji. Dakle, Internet piraterija predstavlja najveću pretnju. Ove Internet lokacije omogućavaju i upload i download piratskog softvera.

Klijent – Server Overuse je kada broj korisnika sa mogućnošcu pristupa server, prekoračuje broj koji je u ugovoru sklopljenom pri kupovini licence.
Hard – disk loading je piraterija u kojoj prodavac računara, odnosno hardvera prodaje hard diskove na koje instalira nelegelne kopije softvera.
Counterfeiting je situacija kada se dupliciranje softvera sprovede tako da se direktno imitira proizvod koji je zaštićen autorskim pravima. Postoji više načina da se softver zaštiti i mada ni jedan nije u potpunosti pouzdan, u stvari služi da bar ljudima stvori što više problema pri nelegalnoj reprodukciji. Navedeni su neki od njih:

• Hardverski orijentisana zaštita – Moćna je, brza i autonomna.
Ova rešenja nude mnoštvo prednosti. Osnovne prednosti su procedura autentifikacije, enkripcija podataka, kontrola pristupa, jedinstveni serijski broj, generator ključa, pouzdanu komunikaciju i identifikaciju uređaja. Ova rešenja se fokusiraju na zaštitu od kopiranja, a neka nude šeme za licenciranje.

Primeri:

- skriveni serijski brojevi – pseudo-nasumično odabrani brojevi skriveni u PC kada je softver instaliran. Korisnik mora da prođe kroz registraciju kako bi koristio program
- medija ograničene instalacije – dozvoljeno je da se softver instalira ograničen broj puta
- dongle – hardverski orijentisani uređaj koji je nakačen na serijski ili paralelni port za štampač. To je ključ koji koristi kodove i lozinke ugrađene u njemu samom koje kontrolišu pristup aplikacionom softveru.

• Softverski orijentisana zaštita – Postoji mnogo ovakvih rešenja. Softverski orijentisana zaštita se lako implementira. Po nekad je jeftinija od hardverski orijentisane zaštite. Prednosti su što se lako koristi, lako se održava, jaka enkripcija i tako dalje.

Primeri:

- FLEXLm – široko korišcen u menadžment tehnologijama. Omogućava da jednom licencom na mreži upravljamo više različitih programa.
- The Protection PLUS – Skup alatki koje omogućavaju da kontrolišemo bezbednost
- IP-Safe – Štiti program licencom

Dakle, postoje pravna i tehnička zaštita. Kod nas, na žalost to ne važi. Pitajući neke naše programere kako štite svoje autorske programe, odgovor je uglavnom bio isti – isčitaju hard disk,

upišu cifre u kod i program će proraditi samo ako prepozna hard disk. Jedan programer se izdvojio po svojoj kreativnosti – laserom je pravio rupu (loš sektor) na flopi disku i zahtevao od programa da pre nego što se pokrene pronađe loš sektor na određenom mestu. Ovo je jedna od najboljih zaštita koje postoje, jer čak i da neko shvati kako je zaštićen program, pa čak i da pronađe gde je loš sektor, trebalo bi da poseduje laser, a onda i da izbuši rupu na istom mestu.

Prema BSA (Business Software Alliance)

1. Više od polovine svetskih kompjuterskih korisnika - 57 % - priznaju da poseduju piratski softver

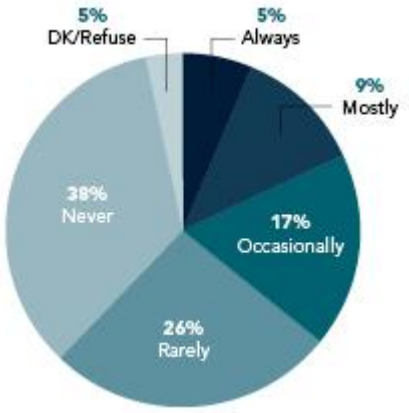
U zavisnsti od zemlje do zemlje, ljudi prijavljuju nelicencirane softvere koja je blisko povezana sa stvarnim stopama piraterije IDC obračunavanja na godišnjem nivou koji se koristi za ovaj izveštaj koristeći tržišne podatke.

2. Globalna stopa piraterije softvera za PC je na 42 %

Ovi korisnici koji kažu da poseduju piratski softver najčešće su neproporcionalni i oni instaliraju više softvera svih vrsta na svojim računarima.

3. Komercijalna vrednost piratskog softvera povećana sa $ 58.8 milijardi dolara u 2010 do $ 63 milijardi dolara u 2011, što je novi rekord, PC pošiljki u ekonomijama u razvoju, gde su stope piraterije najviše.

Ekonomije u razvoju, koji u poslednjih nekoliko godina su bili pokretačka snaga piraterije softvera za računare sada odlučno prevazilaze tržišta u njihovoj stopi rasta. Oni su u 56 % novih svetskih PC isporuka u 2011 i sada čine više od polovine svih računara u upotrebi.[6]



Slika 3. Istraživanje BSA

Istraživanje BSA (slika 3.) je ukratko ustanovljeno sledeće:

- 30% Nikada nije koristilo piratski softver
- 26% Retko
- 17% Povremeno
- 9% Uglavnom
- 5% Uvek
- 5% Odbija

2.2.4 Softverski patenti

U dosadašnjem tekstu, pojam patenta je objašnjena, Međutim, kod softverskih patenata postoji mnogo problema. Iako je za većinu dela, patentirati ih najbolja protekcija, za softver nije. Glavni razlog je to što nakon podnošenja prijave za objavljivanje patenta, do njegovog objavljivanja, može da prođe i nekoliko godina. Pored toga, objavljivanje patenta podrazumeva i objavljivanje tajnih informacija. Takođe je problem i činjenica da ne može svaki softver biti patentiran. Ako bi sadržao bar jedan algoritam koji je već objavljen, ne bi se smatrao inovacijom, a samim tim ni patentom. Patenti mogu da uspore, pa čak i da spreče nove izume. Ovaj fenomen je poznat pod nazivom hold-up problem i pojavljuje se kada pronalazač koji upravo želi da objavi patent, sazna da njegov proizvod ugrožava postojeći patent (Lessing, 2001). Sličan je i problem tragedy of the anticommon. Kod ovog problema se pojavljuje situacija u kojoj svaki stvaralac ima potrebu da se referiše na više priznatih patenata, a da pri tome ne zna koliko će ga vlasnici istih blokirati ili popularno hladiti (Heller i Eisenberg, 1998). Ipak, patentiranje softvera može da pomogne malim kompanijama (kompanijama u osnivanju), da zaštiti svoje programe od gigantskih i već priznatih firmi, koje se u ovakvim situacijama ponašaju kao predatori. U Nemačkoj je u junu 2003, nakon objavljivanja zakona o patentima, sprovedeno istraživanje o tome kako su firme informisane o njemu i koliko ga koriste pri zaštiti softvera. Samo je 6 firmi od 21 koliko je učestvovalo imalo odeljenje za IPR, samo 5 je znalo da zakon postoji. Od istog broja firmi samo je jedna posedovala dva patenta, dok ostale nisu imale ni jedan. To je pokazalo da je i neinformisanost ljudi koji rade u proizvodnji softvera bitan razlog globalne dezorganizovanosti pri ustanovljavanju pravila za zaštitu intelektualne svojine, a samim tim i softvera. Patentiranje, takođe i podiže cenu softvera: treba istražiti postojeće patente, treba sastaviti i podneti prijavu, treba platiti dažbine. U ovakvim uslovima opstaju samo velike kompanije, koje mogu da kompenzuju te troškove obilaznim putevima, a ne direktno preko cene samog softvera. Očigledno je da će se dalja inovacija i proizvodnja pratiti bez hitne intervencije.[5]

Mnogi radovi su napisani na ovu temu. Već izdati patenti mogu da unište savršeno korisne programe. Problem se nalazi u tome što bi svaki programer morao za svaki algoritam pojedinačno da proveri da li je baš taj ikada patentiran da bi bio siguran da ga niko neće tužiti i tražiti naknadu za ono što zaista i jeste njegovo.

2.2.5 Međunarodni problemi po pitanju intelektualne svojine

Postoje dve interesantne stavke u razvoju i internacionalnom IPR zakonu. Prva je inicijativa Sjedinjenih Država da promoviše svoje zakone vezane za intelektualnu svojinu na internacionalnom nivou; druga je uključivanje IPR u TRIPS (trade-related aspects of intellectual property rights). Sporazum i zaključivanje WIPO Copyright Treaty (WCT) (WIPO-World Intellectual Property Organization) je stupio na snagu 2002. godine. WTC se, između ostalog pozabavio zaštitom računarskih programa i originalnih baza podataka, a takođe i armonizacijom nacionalnih zakona vezanih za autorska prava. Patentiranje softvera, ipak nije još uvek harmonizovano, što predstavlja veliki problem. Države Evropske Unije su rešene da ove probleme regulišu i na više sednica EU Komisije su postavljena četiri cilja:

• Harmonizacija nacionalnih IPR zakona
• Ubrzavanje procesa apliciranja za patente
• Adaptacija IPR novim tehnologijama
• Usaglašavanje zakona sa WIPO

Prema Evropskoj konvenciji za patente (Europian Patent Convention) računarski programi kao takvi ne mogu biti patentirani. Ipak, od 1978. godine više od 30000 softverskih patenata je odobreno kao tehnički doprinos odnosno doprinos stanju umetnosti u polju tehnike koji nije očigledan osobi koja je umetnik (Europian Commission 2002.). Patenti mogu da se ostvare u EU na dva načina. Ili da se aplicira Europian Patent Office ili nacionalnoj kancelariji (to naravno ne važi za države koje nisu članice EU). Zbog činjenice da zakon o patentima ne postoji kao evropski, Europian Patent Office ne može da odobri evropski patent. Umesto toga mnogo patenata je odobreno na osnovu Minhenske konvencije pod stavkom Europian Patent iz 1973. godine iz raznih zemalja Evrope. Patenti moraju da budu objavljeni u svim državama članicama.

Da bi ohrabrili patentiranje EU je predložila da se zakoni na nacionalnim nivoima stope sa Minhenskom konvencijom. Po ovome odobreni patenti bi trajali 20 godina uz godišnje obnove koje podrazumevaju i definisane novčane nadoknade. Kao što se vidi, na međunarodnom nivou, patentiranje nije srećno rešeno, ali novi predlozi EU nam daju nadu. Predlog za definiciju grupe patenata koja nas interesuje je izumi koji podrazumevaju upotrebu računara i upotrebu računarske mreže ili bilo koje druge programibilne naprave, odnosno izumi napravljeni da pokreću računarski program ili slične naprave. Izum može biti proizvod (programirani računar) ili procedura. Računarski programi koji su sopstveno vlasništvo autora su zaštićeni zakonima o autorskim pravima. Autorsko pravo je grarantovano vlasniku 70 godina nakon smrti, a onda ga nasleđuju koautori ako ih ima. Novi predlog zakona se odnosi na pirateriju i veća prava vlasnika autorskih prava. Prekršilac bi bio strožije kažnjavan nego li po bilo kom državnom zakonu. U glavnom, u razvijenim zemljama EU i SAD, intelektualna svojina se svela na politiku i takmičenje u industrijskoj nadmoći (novčanim sredstvima), tako da više kreativnost ne dolazi do izražaja već borba pojedinca da zadrži svoje autorsko delo. Većina malih ljudi nije dovoljno snažna da odbrani svoj program, već pored tih radova stoje imena velikih korporacija kao što je Microsoft koje već imaju razrađene sisteme za zaštitu programa. Čak ni ti sistemi nisu dovoljni. Ako kompanija ima ambicije da prodaju svog softvera proširi na druge kontinente, mora da prihvati i pirateriju koja će je još duže vreme obavezno pratiti. U manje razvijenim zemljama,

posebno istočne Evrope i nekim zemljama Azije i Afrike, intelektualna svojina je toliko loše definisana i pravno neregulisana, da osim ove konstatacije nema šta da se kaže.

2.2.6 Zaštita intelektualne svojine u republici Srbiji

Tradicija u zaštiti industrijske svojine na prostoru Srbije duža je od jednog veka. Kraljevina Srbija je bila jedna od 11 država koje su potpisivanjem Pariske konvencije o zaštiti industrijske svojine 1883. osnovale tzv. Parisku uniju. Već 1884. u Kraljevini Srbiji doneti su prvi zakoni iz oblasti zaštite industrijske svojine (zakon o fabričkim i trgovačkim žigovima i zakon o industrijskim mustrama i modelima). Posle Prvog svetskog rata, novonastala država, Kraljevina SHS je, kraljevskom uredbom, 15. novembra 1920. osnovala Upravu za zaštitu industrijske svojine i tako ispunila obavezu iz Pariske konvencije o osnivanju jedne uprave koja ce se baviti priznavanjem prava industrijske svojine i izdavati službeni glasnik u kojem će ta prava objavljivati. Današnji zavod za intelektualnu svojinu je pravni sledbenik te uprave. Nastavljajući pravni kontinuitet prethodnih država i uvažavajući suštinu prava intelektualne svojine, sve države i režimi na prostoru nekadašnje Jugoslavije su oblast industrijske svojine i autorskog prava regulisali na nivou centralne vlasti. Takvo stanje održalo se sve do usvajanja Ustavne povelje državne zajednice Srbija i Crna Gora 4. februara 2003. Tada je došlo do podele nadležnosti, tako da je državna zajednica imala ovlašćenje za donošenje propisa koji će materijalno regulisati pojedina prava intelektualne svojine, dok je sprovođenje tih prava preneto u nadležnost republika članica, odnosno Republike Srbije i Republike Crne Gore. Skupština Srbije i Crne Gore usvojila je u 2004. godini pet novih zakona iz oblasti intelektualne svojine:

1) Zakon o patentima (2. Jula 2004), Zakon o autorskom i srodnim pravima,
2) Zakon o žigovima,
3) Zakon o pravnoj zaštiti dizajna
4) Zakon o zaštiti topografija integrisanih kola (sve 24. decembra 2004) i 2006. godine
5) Zakon o oznakama geografskog porekla.

Ovi zakoni su doneti u postupku potpunog usklađivanja propisa sa zahtevima Svetske trgovinske organizacije, odnosno Sporazuma o trgovinskim aspektima prava intelektualne svojine (TRIPs sporazuma), kao jednog od ključnih sporazuma na kojima počiva Svetska trgovinska organizacija. Svi zakoni usklađeni su i sa odgovarajućim međunarodnim konvencijama kojima je pristupljeno od poslednje velike revizije zakona iz ove materije, koja je obavljena u periodu od 1995. do 1998. godine. Posebno je vođeno računa da novi zakoni budu usklađeni sa odgovarajućim propisima EU. Od 03. juna 2006. Godine Republika Srbija je samostalna država koja i dalje primenjuje ove ranije donete zakone iz oblasti intelektualne svojine.

2.2.7 Intelektualna svojina kao sredstvo ekonomskih integracija

Jedan od zaključaka tzv. „Studije izvodljivosti“ Evropske komisije, koja je prethodila otpočinjanju pregovora o stabilizaciji i pridruživanju EU, je i da zaštita intelektualne svojine i administrativni kapaciteti institucija koje se bave njenim sprovođenjem moraju da budu na nivou standarda EU u trenutku potpisivanja ugovora o stabilizaciji i pridruživanju. Od trenutka kada je „Studija izvodljivosti“ objavljena, zavod i druge institucije, posebno uprava carine, tržišna inspekcija, Viši trgovinski sud i Ministarstvo unutrašnjih poslova, su dosta učinile, ali to još uvek

ne može da se okarakteriše dovoljnim. Još uvek ne postoji nacionalna strategija zaštite intelektualne svojine, specijalizovani sudovi za tu oblast nisu na vidiku, kadrovski kapacitet tužilaštva, carine pa i odeljenja policije koji bi se specijalizovali za povrede prava intelekualne svojine (piratstvo i krivotvorenje robe) nije još uvek dovoljan. Odgovarajuća zaštita prava intelektualne svojine, uključujući ne samo propise već i njihovo brzo, efikasno i kvaliteno sprovođenje, je danas jedan od veoma važnih uslova za bilo kakvu ekonomsku integraciju bilo koje države. Sporazum TRIPS je jedan od tri ključna sporazuma na kojima počiva Svetska trgovinska organizacija, a Republika Srbija očekuje da bi mogli da budu završeni pregovori o pristupanju STO, pri čemu postoje suprotni stavovi i interesi EU i SAD oko nekih bitnih pitanja vezanih za zaštitu intelektualne svojine (geografske oznake, iskjučenja od patentibilnosti, čuvanje tajnih informacija, itd). Sporazum CEFTA je nedavno ratifikovan, a jedan značajan deo sporazuma odnosi se na zaštitu intelektualne svojine i na obaveze koje svaka članica sporazuma preuzima na sebe u sprovođenju te zaštite. Konačno, u postupku pregovora sa EU, jedno poglavlje, od ukupno 35, se odnosi samo na intelektualnu svojinu. Ono što je još bitnije je činjenica da Privremeni sporazum o stabilizaciji i pridruživanju stupa na snagu veoma brzo, nakon usvajanja od strane Evropske komisije i naše ratifikacije, bez ratifikacije u parlamentima svih zemalja clanica EU, a u okviru privremenog sporazuma odredbe koje se odnose na intelektualnu svojinu stupaju na snagu odmah, bez odlaganja. To praktično znači da se pred svim institucijama koje se bave zaštitom intelektualne svojine nalazi jedan veoma odgovoran i ozbiljan zadatak, koji je istovremeno i veliki izazov i velika šansa za te institucije, pa i za zemlju u celini.[5]

2.3 Deset najčešćih pretnji na bazu

Baze podataka imaju najveću stopu oštećenja među svim poslovnim imovinama, prema podacima za 2012 Verizon Kršenje izveštaju. Verizon je obavestio da je 96 % prekršaja su bili prekršaji iz baza podataka, a bezbednosna Fondacija Open je otkrila da 242,6 miliona diskova su potencijalno ugrožena u 2012. Razlog zašto su baze podataka na meti je prilično jednostavan, baze podataka su srce bilo koje organizacije, skladište klijenta i drugih poverljivih poslovnih podataka. Ali zašto su tako ranjivi baze podataka ?, Jedan od razloga je da se organizacije ne štiti ovih sredstava dovoljno dobro. Prema IDC, manje od 5 % od $27 milijardi u 2011 proveo na bezbednosti proizvoda direktno obratio podatke Centar obezbeđenja.[7]

Kada zlonamerni hakeri i insajderi dobije pristup osetljivim podacima, oni brzo mogu da izdvoje (promene podatake) vrednosti, naneti štetu ili poslovanje uticaja. Pored finansijske gubitke ili reputacije, povrede mogu dovesti do kršenja regulatornih, novčane kazne i pravne troškove. Međutim, dobra vest je da većina incidenata - više od 97% prema online poverenje saveza (OTA) u 2013 - Moglo sprečiti primenom jednostavnih koraka i nakon najbolje prakse i unutrašnje kontrole.

Deset pretnji na Bazu podataka : 2010 vs 2013

Ovde imamo prukazano deset najkritičnije pretnje na bazu, prema stavu Imperva Application Center odbrane. U odnosu na 2010 na ovaj novi Izveštaj za 2013 su dodati napadi malwera. Malwer često pokušava da iskoristi mnoge od deset najvećih pretnji, i očekujemo da će se malwer incidenti povećati. Iako nije tehnički pretnja, dodatna je opasnost od nedovoljnog

ulaganja u IT bezbednosti, smatra se na stručnost i obuku radne snage. Organizacije se sve više koristili bazu podataka preko bezbednostne infrastrukture, misleći da će se tako obezbediti.

Ranking	2013 Top Threats		2010 Top Threats
1	Excessive and Unused Privileges		Excessive Privilege Abuse
2	Privilege Abuse		Legitimate Privilege Abuse
3	SQL Injection	↑	Privilege Elevation
4	Malware	NEW	Exploitation of Vulnerable, Miconfigured Databases
5	Weak Audit Trail	↑	SQL Injection
6	Storage Media Exposure	↑	Weak Audit Trail
7	Exploitation of Vulnerabilities and Misconfigured Databases	↓	Denial of Service
8	Unmanaged Sensitive Data	↑	Database Communication Protocol Vulnerabilities
9	Denial of Service	↓	Unauthorized Copies of Sensitive Data
10	Limited Security Expertise and Education	NEW	Backup Data Exposure

Slika 4 Tabela sa deset pretnji

Top deset pretnji :

1. Prekomerna i Neiskorišćeno Privilegija

Kada neko ima privilegije nad bazom podataka koje premašuju zahteve njihove radne funkcije, ove privilegije mogu biti zloupotrebljene. Na primer, bankarski službenik čiji posao zahteva sposobnost da se menja samo accountholder kontakt, informacije mogu da se iskoriste pogodnosti prekomerne zloupotreba baze i povećati račun štednje računu kolege. Dalje, kada neko napusti organizaciju, često njegova ili njena prava pristupa sa osetljivim podacima se ne menjaju. I, da ti radnici odlaze u lošim odnosima, oni mogu da koriste svoje stare privilegije da ukradu podatke visoke vrednosti i nanesu štetu firmi. Kako korisnici završavaju sa prekomernim privilegijama? Obično, to je zato što kontrolni mehanizmi za privilegiju sa ulogama u poslu nisu dobro definisani i održavani. Kao rezultat toga, korisnici mogu dobiti generičke ili standardne pristupne privilegije koje daleko prevazilaze njihove specifične zahteve radnog mesta. Ovo stvara nepotrebne rizike.

2. Zloupotreba privilegije

Korisnici će zloupotrebiti legitimne privilegije baze podataka za neovlašćeno svrhe. interna aplikaciju zdravstvena koja se koristi za pregled pojedinačnih podataka pacijenata preko prilagođenog Web interfejsa. Web aplikacija obično ograničava korisnicima da pregledaju istoriju zdravstvenih rezultata individualnog pacijenta - više zapisa o pacijentu ne može da se posmatraju istovremeno i elektronske kopije nisu dozvoljene. Međutim, lažni korisnik može biti u mogućnosti da zaobiđu ograničenja i povezivanjem na bazu podataka koristeći alternativni klijent kao što je MS - Ekcel. Korišćenje Ekcela i njihove legitimne akreditivnosti za prijavljivanje, korisnik može da preuzme i snimi sve rezultate pacijenta na svoje laptop računare.

Kada zapisi o pacijentu pristignu klijentu, podaci tada postaje osetljiva na širok spektar mogućeg kršenja zakona i privatnosti.

3. SQL Injection

Uspešan SQL injection napad može dati nekome neograničen pristup celoj bazi podataka. SQL injection podrazumeva ubacivanje (ili "ubrizgavanje") neovlašćene ili zlonamerne koda u bazu, u ranjivom SQL podatku, kanalu kao što su Web aplikaciju ili usklađene procedure. Ako se ovo ubrizganje izvrši na bazi podataka, kritični podaci nam postaju dostupni i sa njima možemo manipulisati kako mi želimo. (menjati, brisati…)

4. Malware

Malwer, u prevodu " maliciozni " ili " zloćudni " softver. Osim, klasičnih računarskih virusa obuhvata sve vrste softvera koji na bilo koji način mogu da ugroze računarski sistem ili računarsku mrežu, kao što su trojanci (engl. trojanskih konja), računarski crvi engl. (crvi), rutkit (engl. rootkit), bekdor (engl. backdoor), različite vrste spajwera (engl. špijunski softver), adwera (engl.adware), dajlera (engl. birači), krimwera (engl. crimevare) i dr . štetnog softvera.

5. Slab revizorski trag

Automatizovano snimanje baze podataka koje uključuju osetljive podatke treba da bude deo jedne baze. Neuspeh da prikupi detaljne evidencije, reviziju baze aktivnosti predstavlja ozbiljan rizik organizacije na više nivoa. Organizacije koje imaju slab (ili ponekad i ne postoji) baza podataka revizijoni mehanizmi će se sve više smatraju da su u suprotnosti sa zahtevima industrije i regulatornih vlasti. Na primer, Sarbanes - Oklei (SOKS), koji štiti od računovodstvenih grešaka i malverzacije, a zdravstvenog informacione prenosivosti i odgovornosti Zakon (HIPAA) u sektoru zdravstva, su samo dva primera propisa sa jasnim zahtevima baze revizije. Mnoga preduzeća će se okrenuti domaćim alatima revizije koje pruža svojim bazama podataka proizvođača ili se oslanjaju na ad hoc i ručnih rešenja. Ovi pristupi ne beleže podatke neophodne za podršku revizije, napad, otkrivanje i sudsku odluku. Osim toga, najviše baze podataka revizije mehanizmi su poznati za konzumiranje procesora i diska resursa primorava mnoge organizacije da se smanji ili potpuno eliminiše reviziju. Konačno, većina maternji revizije mehanizmi su jedinstveni za platformu servera baze podataka. Na primer, Oracle stabla se razlikuju od MS-SQL, MS-SQL stabla su drugačiji oblik DB2. Za organizacije sa heterogenim okruženjima baza podataka, nameće značajnu prepreku za sprovođenje jedinstven, skalabilan proces revizije. Kada korisnici pristupaju bazi podataka preko Enterprise Web aplikacije (kao što su SAP, Oracle E-Business Suite, PeopleSoft i) može biti izazovno da shvate šta pristup bazi podataka aktivnost odnosi na određenog korisnika. Većina mehanizama za reviziju nemaju svest o tome ko je krajnji korisnik, jer sve aktivnosti u vezi sa Web aplikacije imenom naloga. Izveštavanje, vidljivost, i forenzička analiza je otežana jer ne postoji veza sa odgovornošću korisnika. Konačno, korisnici sa administrativnim pristupom bazi podataka, bilo legitimno ili zlonamerno dobiti, može isključiti maternji reviziju baze podataka da se sakriju nepoštene aktivnosti. Revizorski zadaci treba da bude idealno odvojen od administratora baze podataka i serverske platforme baze podataka da obezbedi jako razdvajanje dužnosti politike.

6. Skladištenje medija (Backup)

Backup skladištenje medija je često potpuno nezaštićeni od napada. Kao rezultat toga, mnogi bezbednosne štete su uključene kao što su krađa baze podataka, backup diskova. Osim toga, neuspeh na reviziju i praćenje aktivnosti administratora koji imaju nizak nivo pristup osetljivim informacijama možete staviti podatke u opasnost. Uzimajući odgovarajuće mere radi zaštite osetljivih rezervnih kopija podataka i nadgledanje većina visoko privilegovanih korisnika je ne samo najbolja praksa bezbednosti podataka, ali i pod mandatom mnogih propisima.

7. Eksploatacija ranjivih, podešenih baza podataka

Uobičajeno je da se pronađe ranjive i nezaštićene baze podataka, ili otkriti da i dalje imaju podrazumevane naloge i konfiguracioni parametri. Napadači znaju kako da iskoriste ove ranjivosti za napade protiv organizacije. Nažalost, organizacije često se bore da ostanu na vrhu održavanja baze podataka konfiguracije, čak i kada su na raspolaganju zakrpe. To obično traje organizacije meseci da zakrpe bazama jednom patch je dostupan. Za vreme svoje baze podataka su ne zakrpe, oni ostaju ranjive. Prema Nezavisnoj 2012 Oracle grupa korisnika (IOUG), 28 odsto korisnika Oracle nikada nije primenilo kritički Patch Update ili ne znaju da li su oni to uradili. Još 10 odsto uzeti godinu ili duže da prijave svoje zakrpe.

8. Bez upravljanja osetljivim podacima

Mnoge kompanije se bore da održe tačan popis svojih baza podataka i kritične podatke objekte koji se nalaze u njima. Zaboravljene baze podataka mogu da sadrže poverljive informacije, a mogu da se pojave nove baze podataka - na primer, u sredinama Application Testing - bez vidljivosti zaštite. Osetljivi podaci u ovim bazama podataka će biti izložena pretnjama ako su potrebne kontrole i dozvole koje se ne sprovode.

9. Denial of Service

DoS napad i DDoS (Distributed Denial of Service) napad je pokušaj napadača da učini računar nedostupnim korisnicima kojima je on namenjen, on onesposobljava mrežu, računar ili neki drugi deo infrastrukture na taj način da ih korisnici ne mogu koristiti.

Većina DoS napada na internetu spada u jednu od sledeće tri vrste :

A. Napad na ranjive delove mreže - slanje nekoliko poruka na ranjive aplikacije ili operativne sisteme koji se izvršavaju na računaru koji je meta napada i na taj način određena usluga prestaje sa radom
B. Zakrčenje propusnog opsega - pristupni link napadnutog računara postaje zagušen od paketa kojima napadač preplavljuje napadnuti računar čime se sprečava da pravi paketi dospeju na odgovarajući server
C. Pravljenje vezama - napadač uspostavlja veliki broj poluotvorenih ili potpuno otvorenih TCP veza na računaru koji je meta napada i na taj način računar postaje prezauzet lažnim vezama do te mere da prestaje da prihvata ispravne veze.

10. Ograničena stručnost i obrazovanje

Unutrašnje bezbednosne kontrole drži korak sa rastom podataka i mnoge organizacije su slabo opremljeni da se nose za kršenja bezbednosti. Često je to zbog nedostatka znanja potrebna za sprovođenje kontrole bezbednosti, politike i obuke. Prema PVC -a 2012 Information Security prekršajima, ankete je pokazala da 75% anketiranih organizacija iskusnog osoblja u vezi povrede kada je bezbednosna politika slabo shvaćena i 54% malih preduzeća nije imala program za edukaciju svojih kadrova o bezbednosnim rizicima.

Višeslojna baza bezbednosti i Strategijska odbrana

Kao što je pomenuto u prvom delu, prvih deset baznih pretnje se mogu sprečiti primenom jednostavnih koraka i unutrašnje kontrole. Zato što postoji mnogo različitih napada vektora u vezi sa svakom pretnjom, višeslojan odbrambena strategija je neophodna da pravilno zaštitite baze podataka. Tabela ispod identifikuje rešenja za svaki od deset baznih pretnji. Detaljni opisi rešenja su predstavljeni nakon tabele.

	Threat / Solution	Excessive and Unused Privileges	Privilege Abuse	SQL Injection	Malware	Weak Audit Trail	Storage Exposure	Vulnerability Exploitation	Unmanaged Sensitive Data	Denial of Service	Limited Security Knowledge
Discovery and Assessment	Scan for Vulnerabilities			•	•					•	
	Calculate Risk Scores			•				•			
	Mitigate Vulnerabilities			•				•		•	
	Identify Compromised Endpoints				•			•			
	Analyze Risk and Prioritize Remediation Efforts							•			
	Discover Database Servers								•		
	Analyze Discovery Results								•		
	Identify and Classify Sensitive Data	•							•		
User Rights Management	Aggregate Access Rights	•	•								
	Enrich Access Rights Information	•	•								
	Identify and Remove Excessive Rights	•	•		•						
	Review and Approve/Reject Individual User Rights	•									
	Extract "Real" User Identity					•					
Monitoring and Blocking	Real-Time Alerting and Blocking	•	•	•						•	
	Detect Unusual Access Activity	•	•	•	•					•	
	Block Malicious Web Requests			•							
	Monitor Local Database Activity					•					
	Impose Connection Controls									•	
	Validate Database Protocols									•	
	Response Timing									•	
Auditing	Automate Auditing with a DAP Platform					•					
	Capture Detailed Transactions					•					
	Generate Reports for Compliance and Forensics					•					
Data Protection	Archive External Data					•					
	Encrypt Databases						•				
Non-Tech. Security	Cultivate Experienced Security Professionals										•
	Educate Your Workforce										•

Slika5 Pretnje i Rešenje

Bezbednosno definisana rešenja

Postoji šest različitih kategorija rešenja u tablici gore koji su u skladu sa vašom organizacijom i bezbednosnim ciljevima.

1. Otkriće i procena ranjivosti - locirati gde baza podataka i kritični podaci borave
2. Korisničko pravo upravljanja - identifikuje prekomerne prava nad osetljivim podacima
3. Praćenje i Blokiranje - zaštitu baze podataka od napada, gubitka podataka i krađe
4. Revizija - pomaže pokažu poštovanje propisa industrije
5. Zaštita podataka - obezbeđuje integritet podataka i poverljivost
6. Ne- tehničko obezbeđenje - uliva i učvršćuje kulturu svesti o bezbednosti i pripravnosti

1) Otkriće i procena

Skeniranje ranjivosti: Razumevanje ranjivosti kojima je izložena baze podataka na SQL injection je od suštinskog značaja. Malwer može da gleda da iskoriste poznate ranjivosti baze podataka, pravljenje ne-zakrpljene baze podataka i laka meta. Slaba provera pravila mogu omogućiti DoS napada davanjem pristupa bazi podataka bez potrebe za lozinku. Koristite alatke za otkrivanje ranjivosti bezbednosne ranjivosti, i nastalih prodavaca zakrpe. Procene bi trebalo da koristi u industriji najbolje prakse za bezbednost baze podataka, kao što su DISA Stig i ZND merila.

Izračunajte ocenu rizika: ocena rizika na osnovu težine ranjivosti i osetljivosti podataka. Ozbiljnost vrednosti treba da se zasniva na poznatim sistemima kao što je zajednička ranjivost sistema bodovanju (CVSS). Rizika rezultati pomažu pri određivanju prioriteta rizika, upravljanje, a istraživanja ranjivosti. U ovom slučaju, veći rizik rezultata bi se odnosile na SQL injection.

Ublažavanje Slabe tačke: Ako je otkrivena ranjivost i baza podataka prodavac nije izdao zakrpu, virtuelno krpljenje rešenje treba da se koristi. Primena virtuelne zakrpe će blokirati pokušaje da iskoriste ranjivosti bez potrebe za stvarnim zakrpe ili promene na trenutnu konfiguraciju servera. Virtuelno krpljenje će zaštititi bazu podataka od exploit pokušaja dok zakrpa je raspoređena. Opet, fokusiraju na krpljenje visokog rizika ranjivosti koje mogu da olakšaju DOS-a i SQL Injection napad.

Identifikujte kompromitovanih krajnjih tačaka: Identifikovati malwera zaražene domaćini, tako da možete sprečiti ove uređaje da pristupe osetljive informacije u bazama podataka, kao i nestrukturiranih podataka prodavnicama. Kada identifikujete kompromitovanje uređaja, trebalo bi da primenite kontrole osetljivim podacima za ograničavanje tih uređaja da pristupe podacima i ekfiltrating.

Analiza rizika i dati prioritet: Koristite izveštaje i analitičke alate da razumeju rizike i pomažu napore prioritete za sanaciju.

Otkrijte Server baza podataka: U cilju izgradnje i održavanja inventara baza podataka i izolujte osetljive podatke koji se nalaze u njima, organizacije bi trebalo da prvi katalog sve baze

podataka u svojim data centrima. Iskoristite Alatke za otkrivanje da skenira mreže preduzeća i identifikuju aktivne servise baze podataka. Potražite rešenja koja mogu smanjiti trajanje skeniranja filtriranjem na IP adresama i kreće se i do određene usluge (npr. baze podataka Oracle, Microsoft SKL, IBM DB2, itd). Povremeno ponovo pokrenuti otkriće skenira da se identifikuju nove ili promenjene baze podataka.

Identifikovati i klasifikujte osetljive podatke: Kada ste izgradili katalog baza podataka, to je izuzetno važno da se razume koje baze podataka sadrže osetljive podatke. Skeniranje objekata, redove i kolone baze podataka da ukažemo osetljive podatke. Korišćenje podataka rešenja klasifikacija koje imaju u vidu tipova podataka kao što su kreditne kartice, e-mail adrese, brojeva i nacionalni identitet, a koji omogućavaju korisnicima da dodaju prilagođene tipove podataka, kao dobro. Klasifikacija rezultati treba da sadrži IP adresu i ime hosta sredstva, i ukazuju na postojanje osetljivih podataka na tom serveru. Automatski identifikuje osetljive podatke i lične informacije pomažu ograničavanja Bezbednost i usklađenost napora.

2) Upravljanje korisničkih prava

Zbirni Pravni pristup: Skeniranje baze podataka za standardne i privilegovane korisnike, prava i preuzmite detalje kao što su stvarni pravni pristup (npr. SELECT, DELETE, CONNECT, itd), koji su im dali, koji su dobili ta prava, a objekti u kojima su prava dodeljena. Agregiranja korisnička prava u jednu bazu pomaže unapredite izveštavanje i analizu korisničkog pristupa osetljivim podacima.

Obogatite Prava pristupa informacijama sa Detaljima korisnika i podataka Osetljivosti: Dodavanje informacije u vezi sa korisničkih uloga i njihovo ponašanje baze dodaje značajnu vrednost za prava korisnika i analizi pomaže nula-u na zloupotrebe privilegija. Prikuplja i dodajte kontekstualne detalje korisničkih prava informacija, uključujući korisničko ime, odeljenje, objekat baze podataka osetljivosti, i poslednji put pristupa. Ovo vam omogućava da se fokusirate svoju analizu o pravima pristupa koje predstavljaju najveći poslovni rizik. Identifikuju i otklone prekomerne prava i mirno korisnicima: identifikaciju korisnika koji imaju previše privilegije i korisnike koji ne koriste svoje privilegije. Ovo pomaže da se utvrdi da li korisnikova prava pristupa na odgovarajući način su definisani, da razdvajanje dužnosti pitanja, i uklanjanje prekomerne prava koji nisu potrebni za korisnike da rade svoj posao. Hakeri koriste prava pristupa da se predstavi korisnicima i ide za prodavnicama za osetljive podatke. Dakle, smanjenje prekomernog prava štiti od malwera kompromisa.

Razmatra i odobrava / Odbacuje individualna prava korisnika: Obavlja organizovani pregled korisnika prava, kako bi se utvrdilo da li su odgovarajući. Recenzenti treba da odobre ili odbiju prava, ili ih dodeliti drugim za pregled, a administratori mogu da izveštavaju o procesu revizije. Sprovođenje organizovanje korisničkih prava, komentare ispunjava regulativne zahteve i smanjuje rizik, tako što su korisničke privilegije na potrebu da zna osnovu.

Izvaditi "pravi" identitet korisnika: Iskoristite rešenja koji povezuju informacije korisnika sa bazom podataka na kojoj je izvršena transakcija, takođe poznato kao univerzalno Uputstva za praćenje, ili uut. Dobijeni za evidenciju se onda uključuju jedinstvena imena korisnik aplikacije.

3) Praćenje i blokiranje

Uzbunjivanje u Realnom vremenu i Blokiranje: Monitor sve aktivnosti pristupanja bazi podataka i načina korišćenja u realnom vremenu detektuju curenja podataka, SQL neautorizovane transakcije, kao i Protokol i napada na sistem. Kada pokušaji pristupa neovlašćenih podataka se javljaju, generisanje upozorenja ili prekine sednicu za upotrebu. Koristite rešenje kao politika poluge - i unapred definisane običaje - da izvrši inspekciju saobraćaja baze podataka da identifikuje obrasce koji odgovaraju poznatim napadima kao što su DoS napadi, i neovlašćenim aktivnostima. Bezbednosne politike su korisne ne samo za otkrivanje preterane privilegija zloupotreba od strane zlonamernih, kompromitovanih, ili uspavanih korisnike, ali i za sprečavanje većinu od ostalih deset najvećih pretnji baze.

Otkrijti neuobičajene aktivnosti u Access-u: Uspostaviti sveobuhvatan profil, normalnu aktivnost svakoj bazi podataka korisnika. Ove odrednice daju osnovu za otkrivanje DOS-a, Malware-a, SQL injectiona, i neodgovarajućih aktivnosti. Ako bilo koji korisnik zahteva neku akciju koja se ne uklapa u svoj profil, prijavite događaj, generisati upozorenje ili blokirati korisnika. Kreiranje aktivnosti zasnovane na korisničkim profilima povećava verovatnoću otkrivanja neprikladni pristup osetljivim podacima.

Blok zlonamernog zahteva web-a: Zbog Web aplikacije su najčešći vektor za pokretanje SQL Injection napad, prva linija odbrane je da se koristiti zaštitni zid web aplikacija (WAF). WAF će prepoznati i blokirati SQL injection napad, obrasce koje potiču iz Web aplikacija. Za zaštitu od SQL Injection napada, treba WAF :

> Proverite HTTP vrednosti parametara za specijalne karaktere kao što su apostrofi i zagrada i znaju da li su ovi linkovi pravi ili ukazuju na napad.

> Koristite potpise aplikacija i politika poznatih SQL Injection obrazaca upozoravanja i blokiranja.

Nadgledati Aktivnosti lokalne baze podataka: DAP rešenja da nadgledate i prati aktivnosti svojih najvažnijih visoko privilegovanih korisnika - Baza podataka i sistem administratora. Ovi korisnici su dobila najviše nivoe pristupa vašim bazama podataka, oni zahtevaju ovaj pristup radi obavljanja posla. Ukoliko oni zloupotrebljavaju svoje privilegije i postanu ugroženi od strane zlonamernih programa, rizik od krađe podataka i oštećenja vaše organizacije se povećava.

Nametne kontrolu veze: Sprečiti preopterećenosti servera resursima ograničavanjem veze stope, upitu stope, i druge promenljive za svakog korisnika baze podataka.

Proveri protokole baza podataka: Iskoristite aktivnosti baze podataka praćenja rešenja koja se analiziraju protokoli i izoluju slučajnih / anomaliju komunikaciju. Kada se otkriju atipični komunikacionih događaja, rešenje bi trebalo da aktivira upozorenje ili blokira transakciju.

Vreme odziva: Baza DoS napada dizajnirana da resurse preopterećenja servera dovede do odlaganja odgovora baze podataka. Ovo uključuje kašnjenja u pojedinačne upita odgovora i

celokupnog sistema. Koristite rešenja koja prati odgovor merenje vremena i generisanje upozorenja kada sistem reaguje na kašnjenja.

4) Revizija

Automacka revizija sa DAP Platformom: Sprovesti rešenje DAP koji pruža performanse, skalabilnost i fleksibilnost da zadovolji potrebe i najzahtevnijih okruženja. DAP rešenje može da reši većinu slabosti u vezi sa izvornim revizorskim alatima:

> **Razdvajanje dužnosti**: DAP rešenja funkcionišu nezavisno od upravljanja baze podataka, tako da je moguće odvojiti poslove revizije iz administrativnih dužnosti. Pored toga, oni rade nezavisno od servera baze podataka i da su neranjivi na napade visinskih privilegija nisu administratori.

> **Cross - platforma revizije**: DAP rešenja podržavaju platforme baze podataka iz više prodavaca koji omogućavaju jedinstvene standarde i centralizovanje revizionih operacija širom velike i distribuirane heterogenim okruženjima baza podataka.

> **Performanse**: Vodeći DAP rešenja mogu iskoristiti i aparati koji rade na liniji brzinom i imaju nula uticaja na performanse baze podataka. U stvari, prepuštanjem revizije procesa na mrežne uređaje, a ne koristi maternji revizije, organizacije mogu da očekuju da poboljša performanse baze podataka.

Capture Detaljna transakcija: Podržati regulatorne zahteve usklađenosti, napredno utvrđivanje prevara i forenzičke analize, DAP rešenja može da snima evidenciju nadgledanja koji će sadržati podatke kao što su ime izvorne aplikacija, kompletan tekst upita, upit odgovor atribute, izvor OS izvor host ime, i još mnogo toga. Koristite pravila za reviziju da prikupi potrebne informacije potrebne za poštovanje propisa (npr. SOKS, PCI DSS, i Hippa) ili da ispunjava zahteve interne revizije.

Generisanje izveštaja za saglasnost i sudsku medicinu: rezime i format detalji aktivnosti baze podataka u izveštajima koje pomažu ispunjavaju uslova usaglašenosti, sprovođenje forenzičke istrage, komuniciraju vitalne statistike baze aktivnosti i prati performanse sistema. Iskoristite DAP rešenja koja uključuju izveštaje za industriju i državnim propisima koji mogu biti prilagođene potrebama poslovanja.

5) Zaštita podataka

Arhiva Spoljnih podataka: Automatizuje dugoročno arhiviranje procesa. Koristite rešenja koja mogu biti podešena da periodično arhiviranje podataka na eksterno, masovno skladištenje. Podatak bi trebalo da budu opciono zbijen, šifrovan, i potpisan do arhivisanja.

Šifrovanje Baze podataka: Šifrovanje osetljivih podataka u heterogenim okruženjima baza podataka. Ovo vam omogućava da se obezbedi i proizvodnja i rezervne kopije baze podataka, zatim reviziju aktivnosti i kontrolu pristupa osetljivim podacima iz baze podataka korisnika koji pristupaju na operativni sistem i skladištenje nivoa. Po usklađivanje baze podataka reviziju

zajedno sa enkripcijom, organizacije mogu da prate i kontrolišu korisnike i unutar i van baze podataka.

6) Ne-tehnička bezbednost

Negovati iskusnu profesionalnu bezbednost: Da bi se branili od sve većeg niza unutrašnjih i spoljnih pretnji, zaposliti osoblje za bezbednosti informacija koji su dobro upućeni u IT bezbednosti i imaju iskustva u implementaciju, upravljanje i praćenje bezbednosnih rešenja. Kontinuirano obrazovanje i obuka su takođe važni za gajenje dublje bezbednosti znanja i veštine. Takođe i specijaliste za pomoć u realizaciji, sprovođenja bezbednosne procene i penetracija testova, i obezbedi obuku i podršku za svoje administratore.

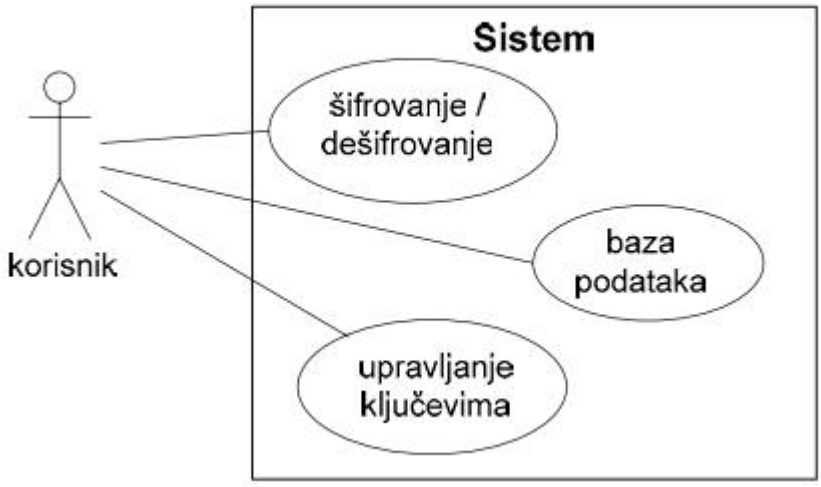
Obrazovati vaše radne snage: Vežbati svoje radne snage na tehnike ublažavanja rizika, uključujući kako da prepoznaju zajedničke sajber pretnje (npr. koplje - phishing napad), najbolje prakse oko korišćenja Interneta i e-mail, kao i upravljanje lozinkama. Propust da se sprovede obuka i stvori " bezbednosnu svesno " kulturu rada povećava šanse za povrede bezbednosti. Krajnji rezultat je dobro obavešteni korisnici koji su obučeni za bezbedno funkcionisanje kada je povezan sa ključnim sistemima.

3. Kriptografska arhitektura

U ovom poglavlju biće razmatrana kriptografska arhitektura, na visokom nivou, za tipičnu aplikaciju koja bi trebala da skladišti šifrovane informacije u bazi podataka. Najveći deo poglavlja razmatra karkteristike ključeva jer bezbednost kriptosistema zavisi od bezbednosti i pažljivog rukovanja ovim ključevima, tako da je odgovarajući prostor posvećen ključevima. Razmatranje obuhvata naglasak na to da bilo koji dati ključ treba koristiti u jednu jedinu svrhu, te da familije ključeva podržavaju taj koncept. Unutar neke familije, ključevi se pomeraju kroz različita stanja onako kako se ti isti ključevi pomeraju kroz svoj radni ciklus. Opseg ključa opisuje kako se primenjuju ključevi unutar sloga baze podataka i određuje kako se rukuje potvrdama o šifrovanju podataka. Koncepti kao što su familija ključa, opseg ključa, radni ciklus ključa, migracija i zamena ključa od fundamentalnog značaja su za razumevanje toga kako funkcioniše baza podataka nekog kriptosistema.[8]

3.1 Osnove arhitekture

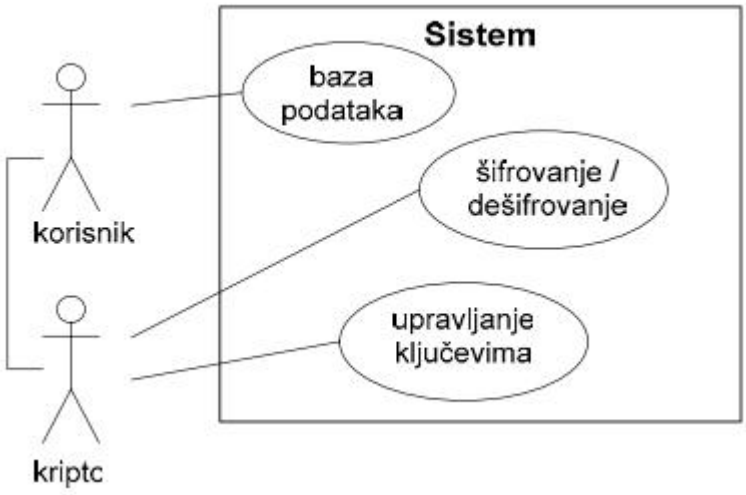
U teoriji razvoja softverskih projekata poznata su dva stila: iterativni i kaskadni stil razvoja. softvera. Prilikom izrade predloga kriptografske arhitekture korišćen je iterativni postupak. Prilikom razvoja baze podataka, koja će poslužiti kao osnova kriptografske arhitekture, pošlo se od modela prikazanog na sledecoj slici 6. U ovom modelu, aplikacija pristupa bazi podataka, šifruje i dešifruje podatke i sama upravlja ključevima. Nedostatak ovakvog modela je očigledan - uloga zaštite podataka i korišćenja podataka je spojena u jednom entitetu.



Slika 6: Jedan entitet u interakciji sa sistemom

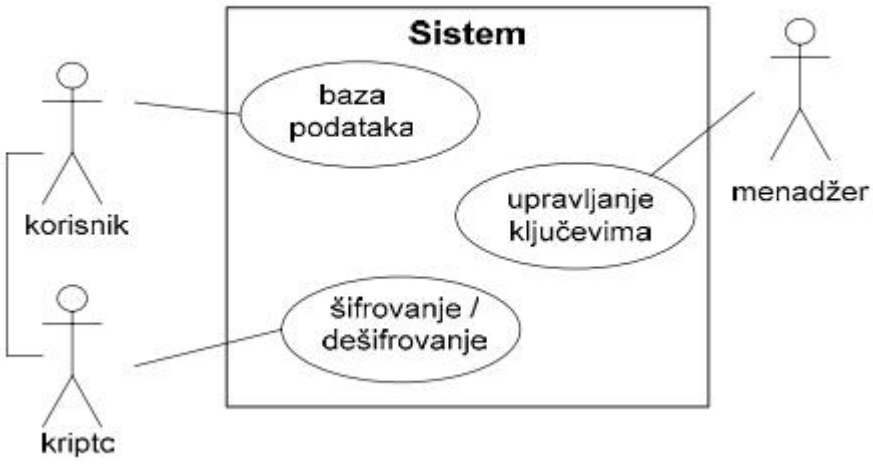
U sledečoj iteraciji, Slika 7: Dva entiteta u interakciji sa sistemom, uloge su podeljene na entitet koji pristupa podacima i na entitet koji šifruje / dešifruje i upravlja kriptografskim ključevima. Ta dva entiteta sarađuju kada korisnik podataka želi da sačuva podatke u bazi (prethodno se

moraju šifrovati) i kada iz baze uzima podatke (podatke je potrebno dešifrovati). Iako ovaj model predstavlja poboljšanje u odnosu na prethodni, nedostaci ipak postoje. Problem je i dalje u vezivanju odgovornosti u jednom entitetu koji upravlja ključevima i kriptografski obrađuje podatke.



Slika 7: Dva entiteta u interakciji sa sistemom

Pored ovog osnovnog nedostatka, predloženi sistem nije modularan. U slučaju proširivanja sistema sa dodatnim kriptografskim modulima, u ovom predloženom modelu, tesno su vezani kriptografski modul sa upravljanjem ključevima. Svaki modul mora "da zna", i da upravlja ključevima, što nije dobro. Na kraju se dolazi do sistema koji je prikazan na sledećoj slici 8:



Slika 8: Finalni model kriptografske arhitekture

Entiteti koji se nalaze u interakciji sa sistemom obuhvataju krajnje korisnike kao što su osoblje za unos podataka ili klijente na Web sajtu i službenike bezbednosti koji su zaduženi za administrativne poslove oko upravljanja ključevima. Osim toga, postoje tipični automatizovani poslovi koji se odnose na unos, obradu i izdvajanje šifrovanih podataka. Da bi se sistem implementirao, odnosno da bi se sa višeg nivoa apstrakcije došlo do konkretnog modela potrebno je analizirati osobine kriptografskih ključeva i njihovu ulogu u celom sistemu. Tada će biti jasnija uloga entiteta i njihova međusobna interakcija.[8]

3.2 Kriptografski ključevi

Kriptografija umanjuje konkretan problem zaštite mnogih tajni na takav način da ovaj postaje problem zaštite samo nekoliko tajni. Taj manji broj tajni predstavlja kriptografske ključeve. Pravilno upravljanje kriptografskim ključevima je od presudne važnosti za uspeh postavljenog cilja, a to je bezbednost informacija. Bezbednost informacija koje se kriptografski štite direktno zavisi od jačine ključeva, efikasnih mehanizama i protokola povezanih sa ključevima kao i od zaštite kojom se štite sami ključevi. Ključevi moraju da se štite od modifikacije, a tajni i privatni ključevi od nedozvoljenog pristupa. Upravljanje ključevima je široka oblast. Razlog tome leži u složenosti sistema koji se pokriva kriptografskom zaštitom, što povlači za sobom veliki broj učesnika u celom razvojnom procesu a oni mogu biti: administratori, programeri, inžinjeri kriptografskih modula, kreatori protokola, kao i administratori zaduženi za bezbednost ključeva. Iz tog razloga biće prikazane one karakteristike ključeva koje su od presudne važnosti za implementaciju kriptografske zaštite baze podataka. Karakteristike koje su obrađene su grupe ključeva i opseg, stanje ključa, trošenje ključa i njegova zamena.

Dužina ključa je posebna karakteristika koja značajno utiče na bezbednost, a koja se odreduje na osnovu algoritma za koji se koristi odredeni ključ. Kako kriptografski algoritmi nisu prikazani u ovom radu neče biti daljeg osvrta na dužinu ključeva.

3.2.1 Odvajanje ključeva

Odvajanje ključeva predstavlja bezbednosni koncept koji nalaže da se određeni kriptografski ključ koristi isključivo u jednu jedinu svrhu. Prednosti odvajanja ključa su sledeće:

– Smanjuje se broj entiteta kojima je neophodan pristup ključu
– Količina podataka koju treba obraditi pri postupku zamene ključa se održava na podnošljivom nivou
– Smanjuje se količina šifrata nastala šifrovanjem datim ključem tako da napadac ima na raspolaganju manje informacija za eventualno razbijanje šifre
– Ograničava se šteta u slučaju da je određeni ključ kompromitovan
– Omogućuje se dizajn različitih nivoa bezbednosti u zavisnosti od različitih podataka koji se štite

Imajući u vidu da bezbednost kriptografskog sistema zavisi od bezbednosti ključeva, najbolje je da se broj entiteta kojima je neophodan pristup ključu održava na apsolutnom minimumu. Ograničavanjem korišćenja ključa u jednu jedinu svrhu, za posledicu ima manji broj entiteta koji pristupaju ključu. U kontekstu kriptografske zaštite baza podataka, ovakva obaveza ograničava upotrebu ključa na samo jednu jedinu bazu podataka. Ključevi se moraju periodicno menjati da

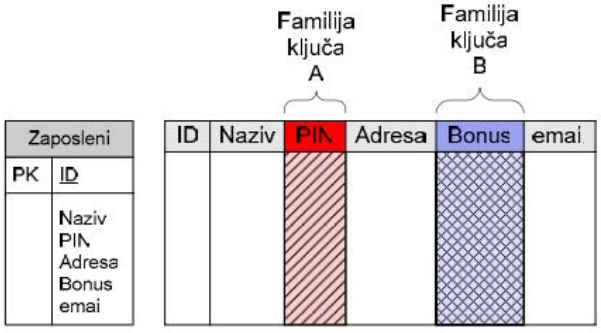
bi bili bezbedni. U toku zamene ključa, svi podaci koji su šifrovni starim ključem se dešifruju i nakon toga se ponovno šifruju ali sa novim ključem. Separacija ključeva može da omogući da ovaj posao bude veoma efikasan, u nekim slučajevima je moguća i paralelna zamena ključeva.

Jedna klasa napada na kriptografski zaštićene podatke, poznatija kao napad pri posedovanju velike količine šifrata (engl. ciphertext attacks), oslanja se na posedovanje velike količine prikupljenih podataka koji su šifrovani istim ključem. Korišćenjem nekoliko istih ključeva ograničava se efikasnost ove klase napada zato što se manja količina podataka šifruje svakim pojedinačnim ključem. U slucaju da eventualno dođe do kompromitovanja nekog od ključeva, sve ono što je šifrovano sa tim ključem takođe se može smatrati kompromitovanim. Odvajanje ključeva ograničava stepen gubitka zato svaki dati ključ štiti samo neke od podataka, a ostali podaci se štite drugim ključevima.

I na kraju, odvajanjem ključeva omogućuje se da snaga zaštite bude prilagođena prema podacima, a ne da se svi podaci štite najvišim stepenom zaštite, trošeći nepotrebno resurse sistema. Npr. ako najveći deo neke baze podataka zahteva upotrebu ključeva dužine 138 bita koji se zamenjuju svaka četiri meseca, a pri tom nekoliko kolona u bazi zahteva upotrebu ključeva dužine 256 bita koji se zamenjuju svakih sedam dana, onda bez upotrebe odvajanja ključa, sve što se nalazi u bazi podataka bi moralo da se ponovno šifruje svakih sedam dana ključem dužine 256 bita. Odvajanje ključa se ostvaruje preko familija ključa i opsega ključa.

1. Familije ključeva

Familija ključa predstavlja jednu grupu ključeva koji se koriste tako da funkcionišu za isti set podataka. Npr. jedna familija se eventualno može koristiti za PIN broj kreditne kartice, a druga za podatke o zdravstvenom stanju. Ključevi se identifikuju imenom svoje familije. Ključevi u familiji imaju specificne uloge koje određuju kako se oni mogu koristiti. Npr. u bilo kom momentu, samo se jedan ključ u nekoj familiji može koristiti za šifrovanje, i dok višestruki ključevi mogu biti korišćeni za dešifrovanje, neka familija često sadrži stare ključeve koji se ne mogu koristiti za šifrovanje ili dešifrovanje. Ovakve uloge se menjaju tokom vremena i o tome se odlučuje na osnovu radnog ciklusa ključa. Najbolja praksa jeste da se odredi jedna jedinstvena familija za svaku kolonu koju je potrebno šifrovati. U slučaju da tabela sadrži pet zaštićenih kolona, idealno je da pet familija budu u stanju da pokriju tabelu. Slika 9: Separacija ključeva, dve familije ključeva prikazuje dve zaštićene kolone pokrivene sa dve familije ključeva.



Slika 9: Separacija ključeva, dve familije kljuceva

Međutim, odnos 1:1 između familija i zaštićene kolone zahteva da svaki ključ bude tako organizovan i primenjivan kako bi se mogao čitati celokupni red. Ovo može da dovede do primetno loših perfomansi. Time što se dozvoljava da odredena familija obuhvati sve kolone donekle se dobija na performansama u administraciji, gde stepen uštede zavisi od toga na koji način se obrađuju kriptografski zahtevi. Čak i kada familija ključeva obuhvata celu tabelu, posebno se šifruje / dešifruje svaka kolona, pa je stoga neophodno izvršiti testiranje implementacije sistema da bi se odredio uticaj familija po kolonama na perfomanse. Često se dešava da su dobici, ako ih uopšte ima, slabi tako da nisu ni vredni žrtvovanja prednosti i dodatne bezbednosti.

2. Grupe familija

Sledeći način za odvajanje ključeva predstavlja korišenje familija ključeva unutar neke kolone. U ovakvom načinu korišćenja familija ključeva potrebno je odrediti kriterijum kojim će se odrediti koja familija se koristi za koji slog. Tako dobijamo tabelu koja je podeljena na "trake", jedna grupa slogova se šifruje / dešifruje jednom familijom, a druga grupa slogova drugom familijom ključeva. Grupe mogu da budu isprepletene ili se mogu nalaziti jedna pored druge, što zavisi od kriterijuma za izbor familije. Slika 10: Grupe familija nad jednom kolonom prikazuje primer grupe familija.

Slika 10: Grupe familija nad jednom kolonom

Npr. ako svaki red tabele bude označen sa jedinstvenim ID brojem, taj broj bi mogao da se iskoristi za određivanje familije. U slučaju da se želi deset familija, familija bi mogla da se računa kao ID modulo 10. U okviru ovakvog scenarija, familije 0 pa sve do familije devet pokrivale bi kolonu, a naknadni novi ažurirani podaci bi upadali u istu familiju zato što se ID kolone ne bi menjao. Ovakav način određivanja familija dovodi do formiranja isprepletenih grupa (pod pretpostavkom da se novi redovi uvek pridodaju tabeli). U slučaju da se za određivanje familije koristi mesec u kome je formiran slog, u tabeli bi bile formirane kontinualne grupe slogova koje čine jednu familiju.

Ovakva strategija može se dalje proširiti tako da višestruke familije takođe pokrivaju višestruke kolone. Deset familija iz prethodnog primera mogli bi da obuhvate nekoliko kolona. Jednostavan slučaj bi zahtevao da sve kolone u datom redu budu pokrivene jednom istom familijom. Da bi ovako nešto funkcionisalo, kriterijum za izbor familije ne sme da zavisi od kolone: bez obzira

koja kolona treba da se šifruje, kriterijumi će na kraju izabrati istu familiju. Pethodni jedinstveni ID kolone i datum kreiranja sloga zadovoljavaju ovakvu karakteristiku.

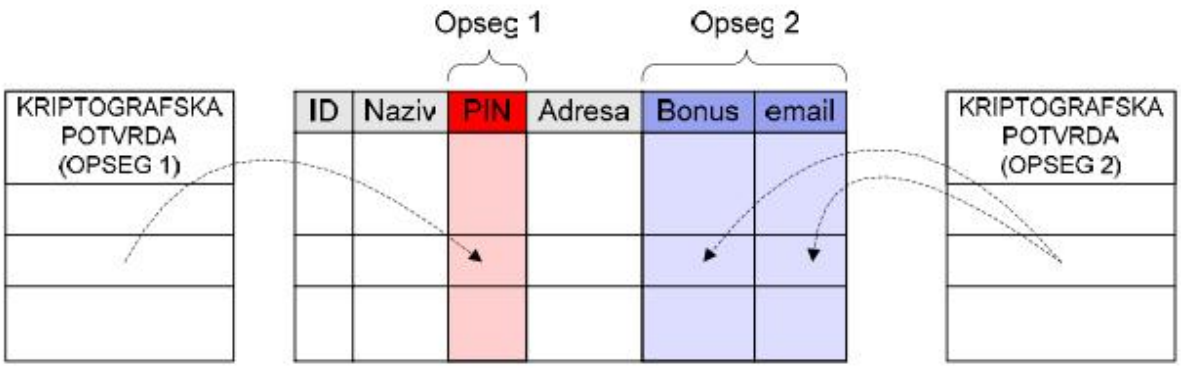
Familija ključa i grupa ključa utiču jedino na šifrovanje novih ili ažuriranih podataka. Dešifrovanje se uvek utvrđuje na osnovu informacije sadržanoj u potvrdi šifrovanja, koja se dobija od kripto modula (Slika 3: Finalni model kriptografske arhitekture), zajedno sa šifratom. U slučaju da dođe do izmene familije dok su podaci šifrovani, ništa se ne dešava sve dotle dok ne dođe trenutak ažuriranja podataka kada je neophodno da se takvi podaci ponovo šifruju. U tom trenutku nova potvrda šifrovanja će ukazivati na neki ključ u novoj familiji.

3. Opseg ključa

Dok familije preslikavaju ključeve u kolone, opsezi ključeva ukazuju na to kako se ključevi koriste radi šifrovanja unutar slogova. Onda kada se slog ubaci u tabelu sa zaštićenim kolonama, potrebno je utvrditi koji ključ ili ključevi su bili korišćeni. Potvrda o šifrovanju koja se dobija od kripto modula sadrži ovakve informacije. U neku ruku, opseg ključa određuje sa kolikim brojem potvrda o šifrovanju korisnik kriptografske usluge mora da upravlja.

Kada je reč o najužem opsegu, svaka zaštićena kolona zahteva svoju sopstvenu potvrdu o šifrovanju. Ovo je slučaj kada se sledi princip najbolje prakse da se koristi jedna familija ključa za jednu kolonu, ali čak i onda kada se koristi samo jedna familija za celu tabelu, ključ može biti uskog opsega. U takvom slučaju, svaka zaštićena kolona se vezana sa svojom potvrdom o šifrovanju. Kod prvobitnog dodavanja sloga u tabelu, sve potvrde o šifovanju će ukazivati na isti ključ. Tokom vremena, međutim, ključevi u potvrdama o šifrovanju će se verovatno razdvojiti dok se pojedinačne grupe podataka ažuriraju, a ostale grupe ostaju neizmenjene.

Ključevi sa uskim opsegom su kompleksniji za upravljanje i zauzimaju više prostora jer čuvaju više potvrda o šifrovanju. Oni su isto tako daleko više fleksibilniji i obezbeđuju bolju bezbednost. Najbolja praksa jeste da se koristi što je moguće uži opseg ključa. Kod najširih opsega, neophodan je samo jedna potvrda o prijemu zbog toga što su sve zaštićene kolone šifrovane jednim ključem. Ovo pojednostavljuje upravljanje ključevima ali ujedno stvara složenije upravljanje prilikom migracije ključeva zbog tog što sve zaštićene kolone treba da budu iznova šifrovane čak i onda kada jedna od njih podleže ažuriranju. Širi opsezi su korisni za grupisanje kolona koje sadrže podatke koji se obično menjaju kao grupa. Npr. broj kreditne karti će i datum njenog isticanja mogli bi da se ubace u zajednički opseg zbog toga što se u slučaju da se jedan od njih menja, onaj drugi će se verovatno isto tako promeniti. Slika 6: Kriptografske potvrde o opsezima prikazuje povezanost opsega sa kriptografskim potvrdama.



Slika 11: Kriptografske potvrde o opsezima

Podaci o kriptografskoj potvrdi se mogu čuvati u istoj tabeli sa podacima ili u nekoj odvojenoj tabeli. Kriptografska potvrda je kompleksan podatak i sadrži minimum šifrat i identifukaciju korišćenog ključa (radi kasnijeg dešifrovanja), a u zavisnosti od korišćenog kriptografskog algoritma i kriptografski materijal kao što je npr. inicijalizacioni vektori. Broj familija koje pokrivaju neku tabelu ne može da bude veći od broja opsega.

Tabela koja ima šest zaštićenih kolona mogla bi da poseduje takvu strukturu da tri kolone pripadaju jednom opsegu, druge dve kolone da pripadaju nekom drugom opsegu, odnosno da preostala kolona bude u svom sopstvenom opsegu. Tada se kaže da tri opsega pokrivaju tabelu.

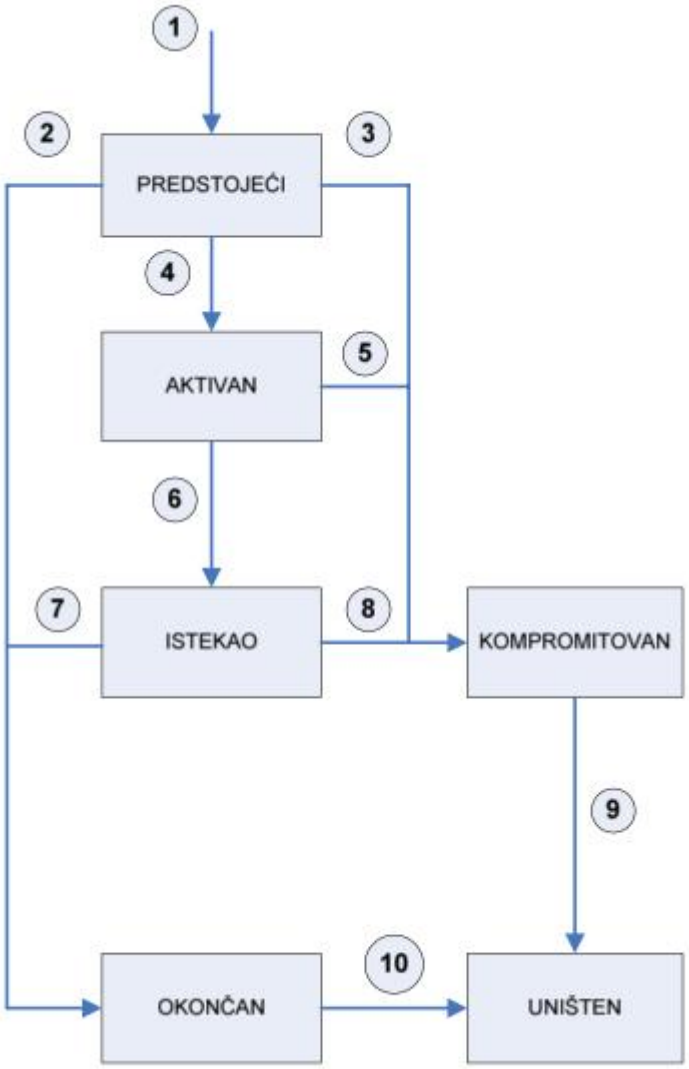
Za tabelu koja je pokrivena sa tri opsega, neophodno je odvojiti smeštaj za tri potvrde o šifrovanju. Tim opsezima se može dodeliti jedna, dve ili tri familije ključa.

3.2.2 Radni vek ključa

Ključevi imaju ograničen vek trajanja. Što više podataka bude šifrovano nekim ključem, takav ključ postaje sve slabiji. Dugi radni ciklus ključa znači da se takav ključ suočava sa većim brojem mogućnosti njegovog kompromitovanja. Takođe, napadač ima više kriptomaterijala kojeg bi eventualno mogao da iskoristi prilikom razbijanja šifre. Da bi se ublažila ovakva inherentna slabost, kriptografski ključevi se periodično moraju menjati. Onda kada se obavlja zamena nekog ključa, svi podaci koji su šifrovani starim ključem moraju biti dešifrovani, a nakon toga se iznova šifruju novim ključem. Zatim se mora obaviti brisanje starog ključa kako se ovaj ne bi iznova koristio. Ključ u svom radnom clikusu može biti u sledećim stanjima :

– predstojeći
– aktivan
– istekao
– okončan
– uništen
– kompromitovan.

Prelaz iz jednog stanja u drugo inicira se događajima kao što je istek kriptoperioda ili saznanje da je ključ kompromitovan. Na sledećoj slici prikazana su stanja u kojima se može naći ključ.



Slika 12: Stanja kljuca sa prelazima

Predstojeći:
Ključ koji postaje aktivan onda kada se javi datum njegovog aktiviranja. Može da postoji nekoliko predstojećih ključeva u okviru jedne familije.

Aktivan:
Ključ koji se trenutno koristi za šifrovanje i dešifrovanje. Može da postoji samo jedan jedini aktivan ključ u okviru neke familije.

Istekao:
Ključ koji je nekada bio aktivan ali je zamenjen novijim aktivnim ključem. Istekli ključevi se koriste za dešifrovanje podataka koji su šifrovani starim ključevima. Može da postoji nekoliko isteklih ključeva u okviru jedne familije.

Okončan:
Neki ključ koje više nije u upotrebi. Može da postoji nekoliko okončanih ključeva u jednoj familiji.

Uništen:
Ključ koji je izbrisan iz trezora. Može da postoji nekoliko uništenih ključeva u okviru jedne familije.

Tabela 2: Dozvoljene kriptografske operacije i stanje ključa ukazuje na one kriptografske operacije koje su dopuštene u svakom od stanja.

Stanje	Šifrovanje	Dešifrovanje
Predstojeći	Ne	Ne
Aktivan	Da	Da
Istekao	Ne	Da
Okončan	Ne	Ne
Uništen	Ne	Ne

Tabela 4: Dozvoljene kriptografske operacije i stanje ključa

Po formiranju ključa, dodeljuje mu se familija i datum aktiviranja. Datum aktiviranja ukazuje na datum kada takav ključ prelazi u aktivno stanje. Sve dok ne dođe taj datum, takav ključ se nalazi u predstojećem stanju i ne može se koristiti za kriptografske operacije. Posle datuma aktiviranja ključa, ključ postoje aktivan i bilo koji prethodno aktivan ključ u familiji se na taj način prebacuje u stanje isteka. Aktivno stanje je jedino stanje koje omogućuje šifrovanje i svi zahtevi za šifrovanjem unutar neke familije ključeva koristi ključ koji je u toj familiji aktivan.

Ključevi u stanju isteka se nikada više ne koriste za šifrovanje. Ključ koji je istekao može se isključivo koristiti za dešifrovanje podataka koji su šifrovani onda kada je ključ bio aktivan. Stanje isteka je u suštini stanje zadržavanja sve do onog trenutka kada se ključ može zameniti. Najbolje je zameniti ključeve što pre je to moguće, kako on u stanju isteka ne bio bio duži vremenski period.

Kada se jednom svi podaci koji su bili šifrovani nekim ključem isteka ponovno šifruju sa novim ključem, ključ isteka bi trebalo postaviti u stanje okončanja. Stanje okončanja ukazuje da ključ više nije u upotrebi ali da i dalje postoji u trezoru za ključeve. Razlika između stanja okončanja i uništenja je u tome što je uništen ključ izbrisan iz trezora za ključeve. U oba ova slučaja, ključ se ne može upotrebiti. Najbolje bi bilo da se iz trezora za ključeve izbriše kad dođe u stanje okončanja što je pre moguće. čak i oni ključevi koji se više ne koriste predstavljaju rizik zbog toga što bi napadač eventualno mogao da dođe u posed šifrovanih podataka koji su šifrovani takvim ključem. Nemarno rukovanje ključevima u stanju okončanja može lako da dovede do

kompromitovanja podataka. Uobičajni princip koji se odnosi na celokupni radni ciklus ključa jeste da ključevi ne bi trebalo da se nalaze u bilo kom od pomenutih stanja duže nego što je to neophodno. Čim neki ključ dođe do kraja svog predviđenog operativnog perioda u nekom od pomenutih stanja, trebalo bi da se pomeri u sledeće stanje. Na sličan način, kada je reč o predstojećim ključevima, najbolje bi bilo da se ključevi ne formiraju za isuviše dug vremenski period unapred. Cilj je da se ključevi koriste za što je to moguće najkraći period vremena. Što je ključ duže u upotrebi, veće su mogućnosti njegovog kompromitovanja.

3.2.3 Zamor ključa

Prilikom određivanja familije i opsega ključa, potrebno je uzeti u obzir količinu podataka koju treba da zaštiti neki ključ kako bi se suprotstavili mogućoj pretnji izlaganja informacija. Izlaganje informacija ukazuje na mogućnost dolaska do otvorenog teksta uz pomoć šifrata slabe prisutne tragove otvorenog teksta koji je i dalje tu i tamo očuvan u šifratu. Dok se sve više podataka šifruje uz pomoć nekog ključa, to je više verovatno da će šifrovanje izazvati izlaganje otvorenih informacija kroz šifrat, i stoga sistem mora da ograniči količinu podataka koja se šifruju takvim ključem. Analiza isticanja informacija opisana je u okviru bibliografskih podataka i obezbeđuje odlično uputstvo o tome kako da se odredi ova granica i stoga se posebno preporučuje. Kada se jednom stigne do granice, verovatnoća isticanja informacija postaje gotovo sigurna. Ključ je u suštini u fazi “zamora” i njegova dalja upotreba smanjuje bezbednost. Iz ovih razloga je potrebno odrediti kriptoperiod. Kriptoperiod je vremenski okvir u kome je dozvoljeno korišćenje ključa od strane legitimnih korisnika. Prikladno određen kriptoperiod:

– ograničava količinu podataka koja se štiti datim ključem i time smanjuje kolicinu šifrata dostupnu kriptoanalizi
– ograničava količinu podataka dostupnih napadaču u slučaju kompromitovanja ključa
– ograničava se korišćenje određenog algoritma na njegovo predviđeno vreme upotrebe
– organičava se vreme pokušaja narušavanja fizičkih, logičkih i proceduralnih mehanizama kojima je ključ zaštićen od napada
– ograničava se vreme za procesorski intezivnu kriptoanalizu.

Nekada se kriptoperiod ograničava u terminima vremena ili sa maksimalnom količinom podataka koja se štiti ključem. Kriptoperiod je potrebno pažljivo odrediti jer se lošom procenom rizikuje izlaganje ključa neautorizovanoj strani. Postoji mnoštvo faktora rizika koji uticu na mogućnost izlaganja ključa i neki od njih su:

1. jačina kriptografskih mehanizama (npr, algoritam, dužina kljuca, velicina bloka i mod u kome radi sistem),
2. vrsta implementacija kriptografskog mehanizma(npr. implementacija po standard FIPS 140-2 Nivo 4 ili softverska implementacija na personalnom racunaru),
3. radno okruženje (e.g., zašticeno okruženje sa kontrolom pristupa, poslovni prostor ili javno dostupni terminal),
4. količina informacija ili obavljenih transakcija,
5. životni ciklus samih podataka,
6. bezbednosna funkcija (šifrovanje, digitalni potpis, generisanje kljuceva, zaštita kljuceva),

7. metod unosa ključa (korisnik unosi ključ tastaturom, uz pomoć drugog ključa, korišćenjem uređaja, udaljeno uz pomoc PKI),
8. proces zamene ili generisanja ključa,
9. broj čvorišta mreže koji dele zajednički ključ,
10. broj kopija ključa i distribucija kopija
11. pretnja po podatke (od koga se želi postići zaštita, koliku tehničku i finansijsku moć ima napadač).

Generalno gledano kratki kriptoperiod znači da je bezbednost na većem nivou. Međutim, ako se proceni da postoji opasnost od ljudske greške pri zameni ključeva onda će česta zamena ključeva da poveća opasnost po same podatke. Ponekad je bolje koristiti kurirsku distribuciju ključeva koja nije česta, posebno ako se radi o asimetričnom kriptografskom sistemu.

3.2.4 Migracija ključa

Prilikom ažuriranja podataka koji su već šifrovani, ako se ključ kojim su ti podaci šifrovani nalazi u fazi isteka, dolazi do procesa koji se naziva migracija ključa. U takvoj situaciji, podaci se dešifruju uz pomoc kljuca u fazi isteka, a promene nad podacima se šifruju uz pomoć aktivnog ključa.

Prilikom migracije treba biti oprezan, jer ako se koristi široki opseg ključa – pokriva veći broj kolona, čak i ako bude ažuriran podskup kolona koji se nalaze u okviru nekog opsega, sve kolone opsega moraju da budu podvrgnute migraciji. To je zbog toga što se u potvrdi o šifrovanju nalazi identifikacija ključa koja važi za ceo opseg.

Uski opsezi u potpunosti sprečavaju nastanak ovakve situacije zbog toga što svaka kolona poseduje svoju sopstvenu potvrdu o prijemu. Isto tako ažurno zamenjivanje ključeva koji su došli u fazu isteka smanjuje frekvenciju migracija ključa, a ključevi koji ističu zato što su došli do kraja svog korisnog radnog ciklus, trebalo bi zameniti što je to pre moguće.

3.2.5 Zamena ključa

Zamena ključa je postupak zamene ključa u fazi isteka novim aktuelnim aktivnim ključem. Proces zamene zahteva da se podaci koji su šifrovani sa ključem u fazi isteka dešifruju i da se zatim obavi ponovno šifrovanje sa novim aktivnim ključem. Kada jedanput svi podaci budu iznova šifrovani, ključ u fazi isteka trebalo bi da dobije oznaku ključ u fazi povučenosti kako bi se naznačilo da ovaj ključ više nije neophodan.

Najbolja praksa ograničavanja jedne familije na jednu kolonu pojednostavljuje zamenu ključa. U takvom slučaju, neophodno je ispitati samo jednu jedinu kolonu radi prisustva ključa u fazi isteka, tako da se minimizirati rizik od slučajnog propusta da je u upotrebi ključ koga više nema. Što je više kolona koje pokrivaju neku familiju, posebno ako se takve kolone nalaze u različitim tabelama, to je veći rizik da jedna od njih bude izgubljena, najčešće zbog nedokumentovanog ažuriranja kriptografske šeme.

Rizik gubitka podataka u nekoj fazi ažuriranja nosi sa sobom ozbiljne posledice zato što je ključ u fazi isteka povučen, i uskoro se kao takav briše u trezoru za ključeve. Dok ključevi koji su

izbrisani u trezoru za ključeve možda i mogu da se dalje zadrže u bezbednoj, offline arhivi, teško je obaviti dešifrovanje na osnovu tako arhivisanih ključeva. U slučaju da ključ bude sklonjen čak i iz arhive, svi podaci koji ostaju šifrovani takvim ključem se u principu izgubljeni.

Ključ koji dolazi u fazu isteka trebalo bi zameniti što je pre moguće. Što duže ključ ostaje u sistemu, veći je rizik da takav ključ bude kompromitovan. Međutim, zamena ključa troši dosta procesorske snage imajući u vidu da se dešifruje velika količina podataka, a zatim se obavlja ponovno šifrovanje u relativno kratkom vremenskom periodu. Ti troškovi prilikom česte zamene ključa mogu da budu preterano visoki. Zamena kjuča isto tako dovodi do uvođenja dodatne administracije, uključujući tu konfigurisanje i arhiviranje ključeva.

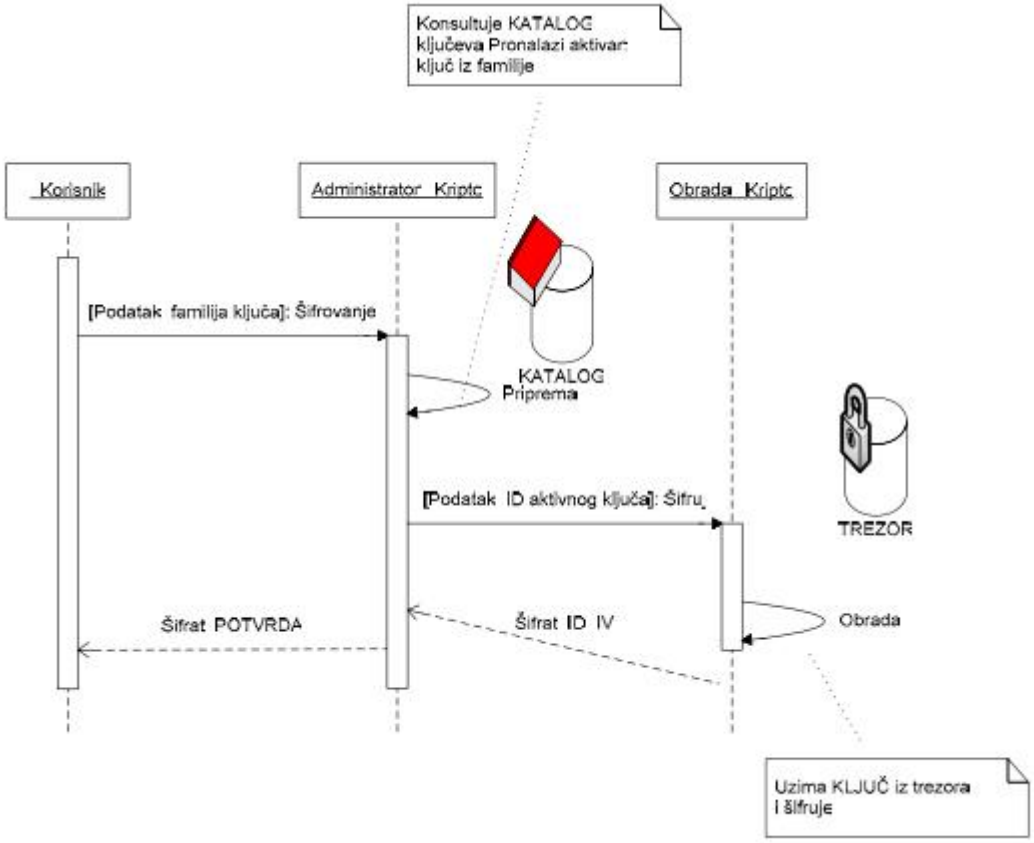
Zamena ključa u toku jedne godine u toku koje se javlja faza njegovog isteka je razuman potez. U slučaju da je ključ aktivan za period od jedne godine i nakon toga njegova faza isteka se odvija sledeće godine, tada je kompletan operacioni period ovakvog ključa dva (dve godine). Dve godine je dugački vremenski period za nekog napadača da može da smisli napade na trezor za ključeve, podršku za ključeve, ili procedure administracije za ključeve. U slučaju da je ključ zaštićen u nekom hardverskom uređaju koji je imun na malverzacije, onda bi moglo biti razumno da se produži stanje isteka (Expired state) na dve godine.

3.3 Predlog rešenja

Posle analize osobina kriptografskih ključeva i njihove uloge u sistemu zaštite baze podataka dolazi se do fizickog modela baze podataka koja podržava pomenute zahteve i ograničenja spomenuta u prethodnim poglavljima. Da bi predloženi fizicki model bio jasniji sledi prikaz interakcije izmedu pojedinih komponenti sistema sa slike 3.

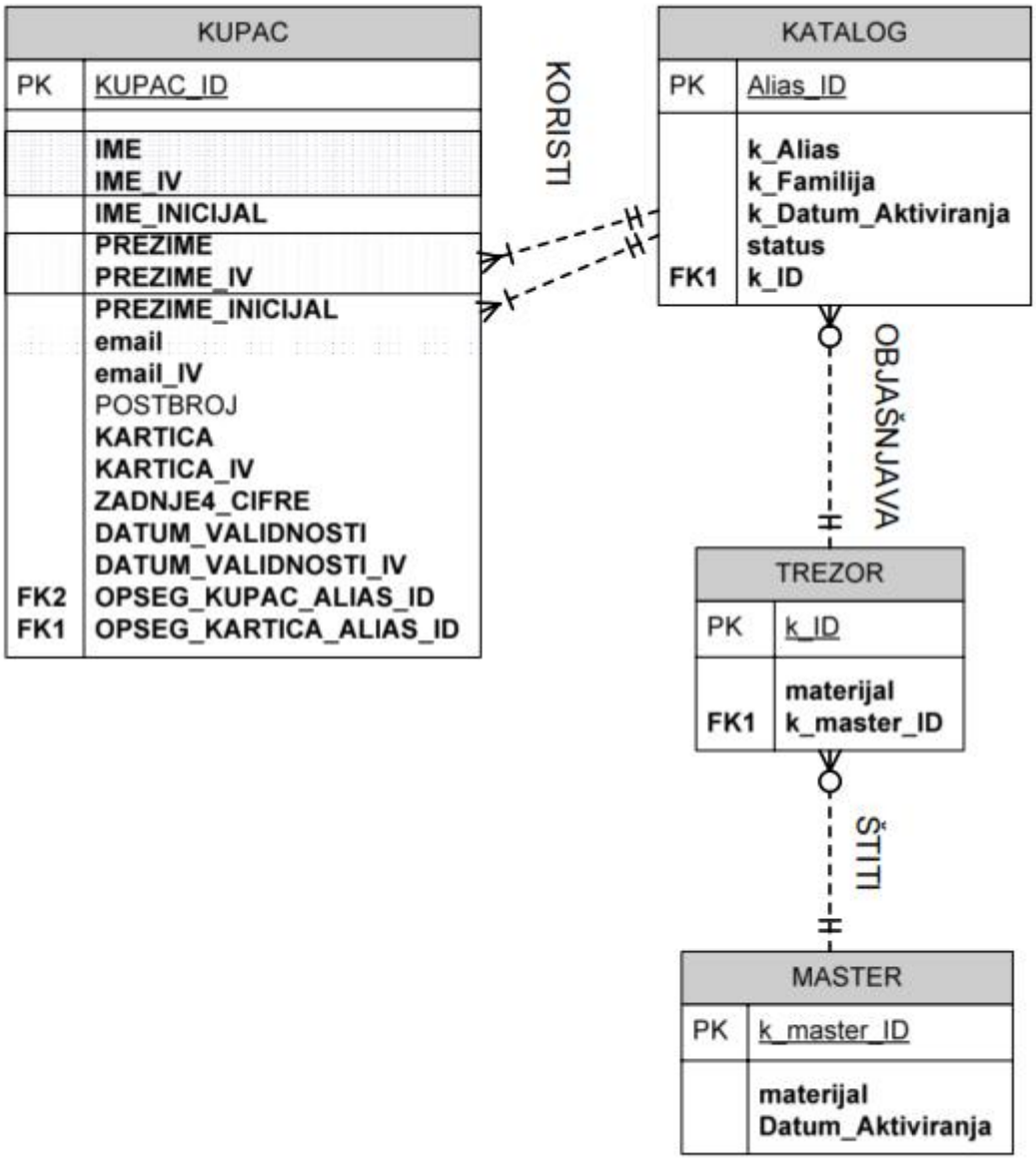
Korisnik je zainteresovan za podatke. Želi da podatke smesti u bazu, te da oni u bazi budu šifrovani i da prilikom uzimanja podataka iz baze oni budu dešifrovani. Mora da poznaje koju familiju ključeva će koristiti za zaštitu podataka. Takode posle dobijanja šifrovanih podataka, zajedno sa šifarskom potvrdom, te podatke mora da sačuva, u suprotnom neće biti u stanju da dešifruje podatke. U slucaju da se šema baze podataka izmeni i modul Korisnik će pretrpeti velike izmene.

Kripto modul se sastoji iz dva dela. Jedan deo prima zahtev od Korisnika. Dobija podatak koji treba šifrovati zajedno sa identifikacijom familije iz koje treba uzeti aktivan ključ. Informacije o ključevima, ali ne i sami ključevi, se nalaze u katalogu ključeva. U katalogu ključeva, pronalazi identifikaciju aktivnog ključa za traženu familiju ključa i priprema odnosno generiše dodatne potrebne podatke kao što je inicijalizacioni vektor. Sve to šalje delu kriptografskog modula zaduženog za šifrovanje. On, na osnovu identifikacije ključa pronalazi odgovarajuci ključ u trezoru sa ključevima, šifruje podatke, a šifrat sa šifarskom potvrdom šalje delu koji komunicira sa korisnikom. Razdvajanje Kripto modula na dva dela je potrebno zbog veće sugurnosti, tako što deo koji komunicira sa korisnikom nema pristupa trezoru sa ključevima. Isto tako, deo koji šifruje / dešifruje podatke pristupa trezoru sa ključevima ali samo da bi iz trezora uzeo kljuceve. Odgovornost za kreiranje i uklanjanje ključeva iz trezora je nadležnost Menadžera ključeva.



Slika 13: Dijagram sekvenci za proces šifrovanja

Menadžer ključeva je modul čiji je zadatak da kreira, uklanja ili menja ključeve. Ima pristup Katalogu ključeva i samom Trezoru sa ključevima. Iz razloga sigurnosti, a poštujući princip deljene odgovornosti, Menadžer ključeva ne može da koristi kripto modul, i obrnuto. Kripto modul ne sme da kreira ili modifikuje ključeve. U celom sistemu, ova komponenta ima jednu od najosetljivijih uloga. Sledeća slika prikazuje deo fizickog modela baze podataka za podršku upravljanja ključevima.



Slika 14: Fizicki model BP za podršku upravljanja ključevima

4. Primer Zaštite Access baze podataka

Microsoft Access je Microsoftow program za upravljanje relacionim bazama podataka. Sastoji se od Microsoftovog mehanizma " Džet " za baze podataka (engl. Microsoft Jet Database Engine) i grafičkog korisničkog okruženja. Deo je programskog paketa pod nazivom Microsoft Office. Takođe, može se kupiti i odvojeno. Ne postoji verzija za [Mac OS] niti za Windows Mobile platformu.[8]

Access sprema podatke baze u vlastitom formatu - Access Jet Databease Engine. Isto tako, može prebaciti ili ostvariti vezu sa podacima u drugoj Access bazi ,Excelu, Share Point listama, tekstom, XML-om, Outlooku, formatu dBaseu, Paradoxu, Lotusu 1-2-3 ili pomoću ODBC izvora podataka kao što su Microsoft SQL Server, Oracle, MySQL i PostgreSQL. Access koriste profesionalci za razvoj aplikacija, ali ga jednako tako mogu koristiti i amateri, power useri za razvoj jednostavnijih aplikacija. Access podržava pojedine tehnike objektno orijentisanog programiranja, ali se ne smatra objektno orjentisanim alatom.

Microsoft Access je deo programskog paketa Microsoft Office i najpopularnija je Windous baza. Namenjena je korisnicima koji imaju potrebu za relacionim bazama podataka, a Ekcel, odnosno Excelove baze, liste i izvedene tabele su jednostavno preslabe.

4.1 Istorijat

Access, verzija 1.0 razvijena je u oktobru 1992. godine, a ubrzo je izašla verzija 1.1 u maju 2003. koja je imala Access Basic programski jezik i bolju kompatibilnost sa ostalim programima iz paketa Microsoft Office.

Microsoft je naveo zahteve za Access 2.0: Microsoft Vindovs 3.1, 4 MB RAMa, 6 MB RAMa preporučeno, 8 MB prostora na čvrstom disku, 14 MB preporučeno. Proizvod se isporučivao na sedam 1.44 MB disketa. Uputstva su izašla 1993. godine.

Access je relativno dobro radio s malim bazama podataka, ali pod određenim okolnostima moglo je doći do narušavanja konzistentnosti podataka. Tako su npr. baze preko 10 MB bile problematične (treba imati na umu da su u to vreme hard diskovi većinom bili ispod 500 MB), a u uputstvima su bile pobrojane okolnosti u kojima može doći čak do gubitka podataka. Kako bi to rešio, Microsoft je izdao 8 - Service Packova za svoj Jet Database Engine i stvari doveo u red.

Pojavom Microsoft Office 95, Access 95 postaje delom programskog paketa Microsoft Office Professional uz zamenu jezika Access Basic u višu Basic for Applications (VBA). Nakon toga nova verzija Accessa izlazi kad i nova verzija programskog paket Microsoft Office. To znači Access 97 (verzija 8.0), Access 2000 (verzija 9.0), Access 2002 (verzija 10.0), Access 2003 (verzija 11.0) i Access 2003 (verzija 12.0).

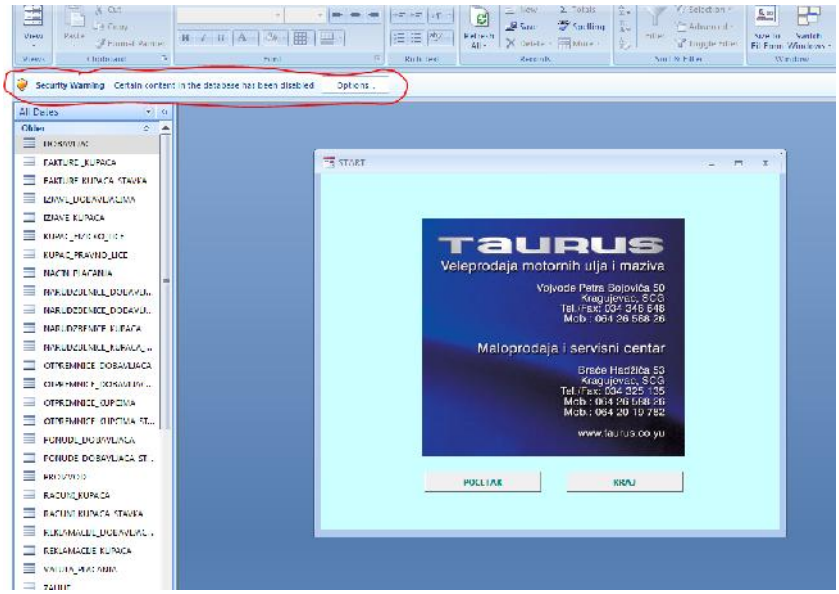
Format baze Access (Jet MDB) je takođe evoluirao tokom godina. Format egzistira u Accessu 1.0, 1.1, 2.0, 95, 97, 2000, 2002, i 2007. Najveća promena u formatu baze podataka napravljena

je u verziji Access 2000 koji nije kompatibilan unazad, odnosno sa starijim verzijama formata, Access 97 i starijima. Sve sadašnje verzije Accessa podržavaju format iz Accessa 2000. Nova svojsta dobio je format baze za Access 2002 i one se mogu koristiti u verzijama Access 2002, 2003 i 2007. U Accessu 2007 predstavljen je novi format baze podataka, accdb. Accdb format podržava više vrednosne podatke i priloge poljima. Ti novi tipovi podataka omogućavaju unos više vrendosti u jedno polje.

Pre pojave Accessa tržištem desktop, stonih baza podataka vladao je Borland, sa svojom bazom Paradok, dBase i FokPro. Access je prva masovna baza podataka za Windous OS. Kupovinom Fok Proa i ugradnjom optimizacije upita u Access, Microsoft Access ubrzo postaje dominantna baza pod Windovsima pomevši konkurenciju koja još nije napravila tranziciju sa DOS-a. Access se u početku zvao Cirrus, a forme Rubi. Pre Visual Basica Bill Gates je vidio prototip i odlučio da će se [Basic] razvijati posebno, projekat je nazvan Thunder. Ta dva projekta su se razvijala svaki posebno i forme im nisu bile kompatibilne. To je rešeno uvođenjem jezika VBA Access je bio naziv komunikacionog programa koji je trebao biti konkurencija programu [Pro Comm] i ostalim sličnim programima. Projekat je propao i godinu dana kasnije Microsoft koristi naziv Access za svoju bazu podataka.

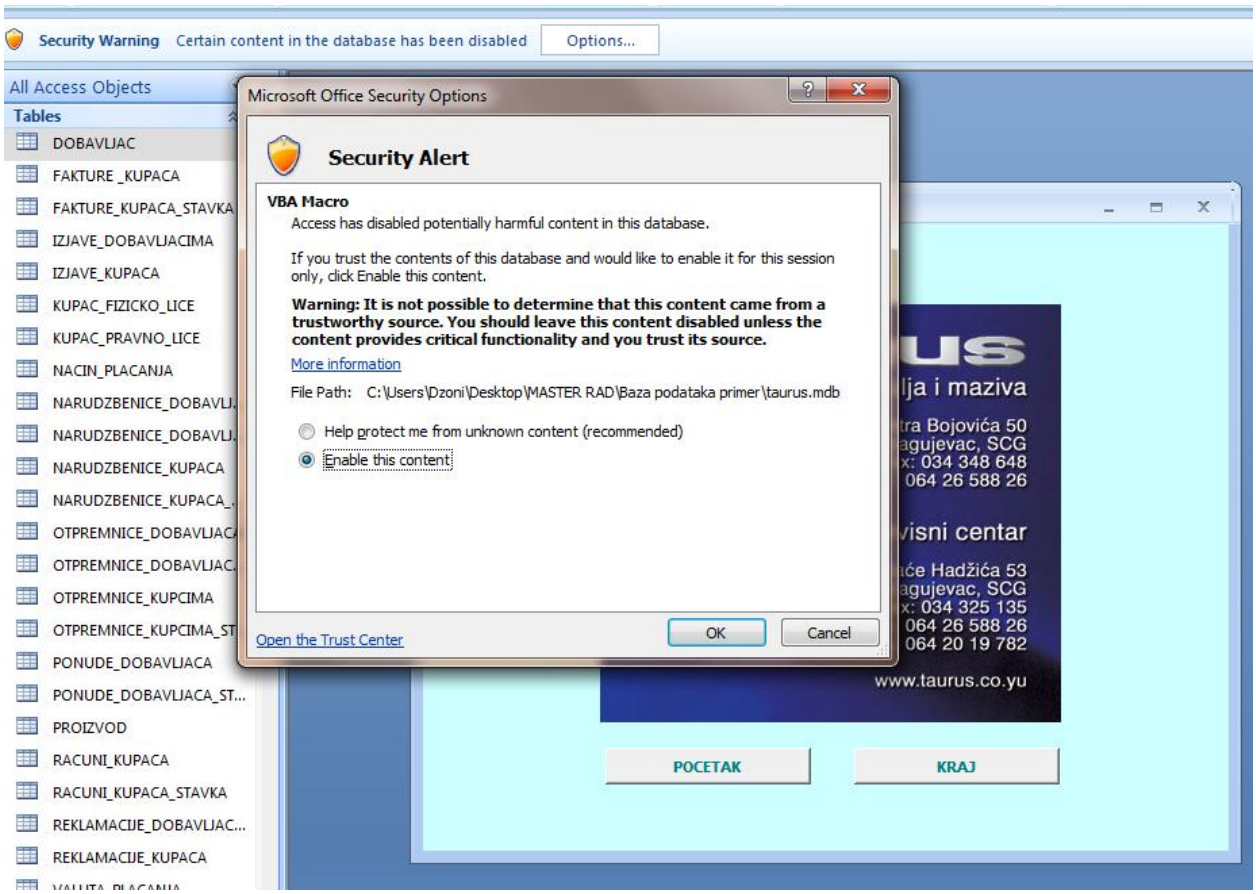
4.1 Access Bezbednosno upozorenje

U prethodnim verzijama programa Access, kada bi smo kreirali bazu morali smo da napravimo niz izbora. Na prime, morali smo da biramo između nivoa bezbednosti (nizak, srednji ili visok), da li želimo da pokrenemo potencijalno nebezbedni kod ili ne. Više ne moramo da donosimo takve odluke kada otvorimo bazu podataka u programu Access 2007. Podrazumevano, Access 2007 onemogućava sve potencijalno nesigurni, bez obzira na verziju programa Access koju smo koristili za kreiranje baze podataka. Dakle možemo onemogućiti prikazivanje dela ili svih objekata u bazi podataka. (slika 15)



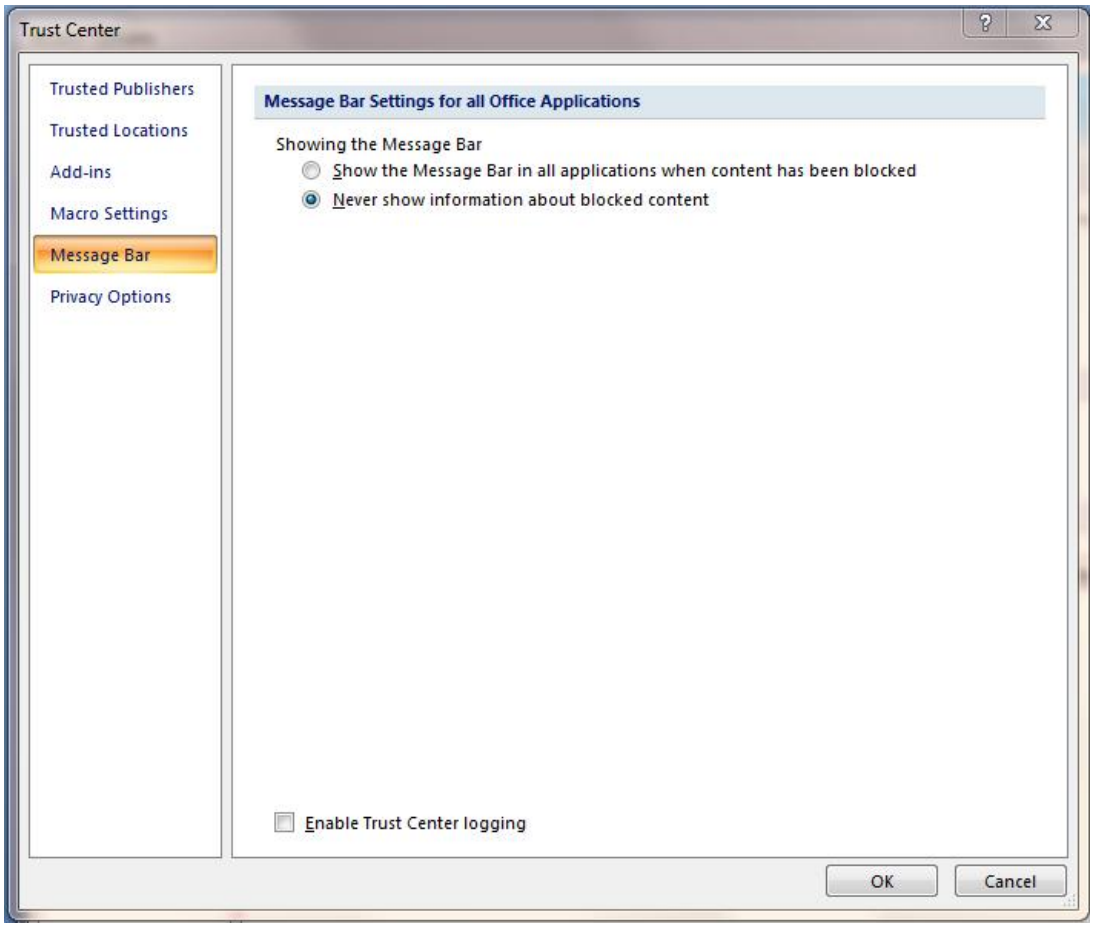
Slika15 Izgled Obaveštenja

Ukoliko čekiramo ” Enable the content ” odn. Omogući sadržaj, pristupićemo bazi sa neograničenim pristupom ali taj pristup će trajati sve dok ne isključimo bazu i pokrenemo ponovo, opet će nas čekati upozorenje.



Slika 16 Security alert

Ali ako se odlučimo da čekiramo “ Help protect me from unknown content “ koji se inače preporučuje, pristupićemo bazi ali sa ograničenim pristupom. Ukoliko ne želimo da nam se ovo upozorenje prikazuje ubuduće, kliknemo na “ Open the Trust Center “, gde će nam se pojaviti sa leve strane meni na kojem se pored ostalih nalazi Message bar, i kada kliknemo na njega nama će se postaviti Showing Message Bar gde nam je ponuđeno da čekiramo “ Prikaži poruku ili Nikada ne prikaži poruku” .



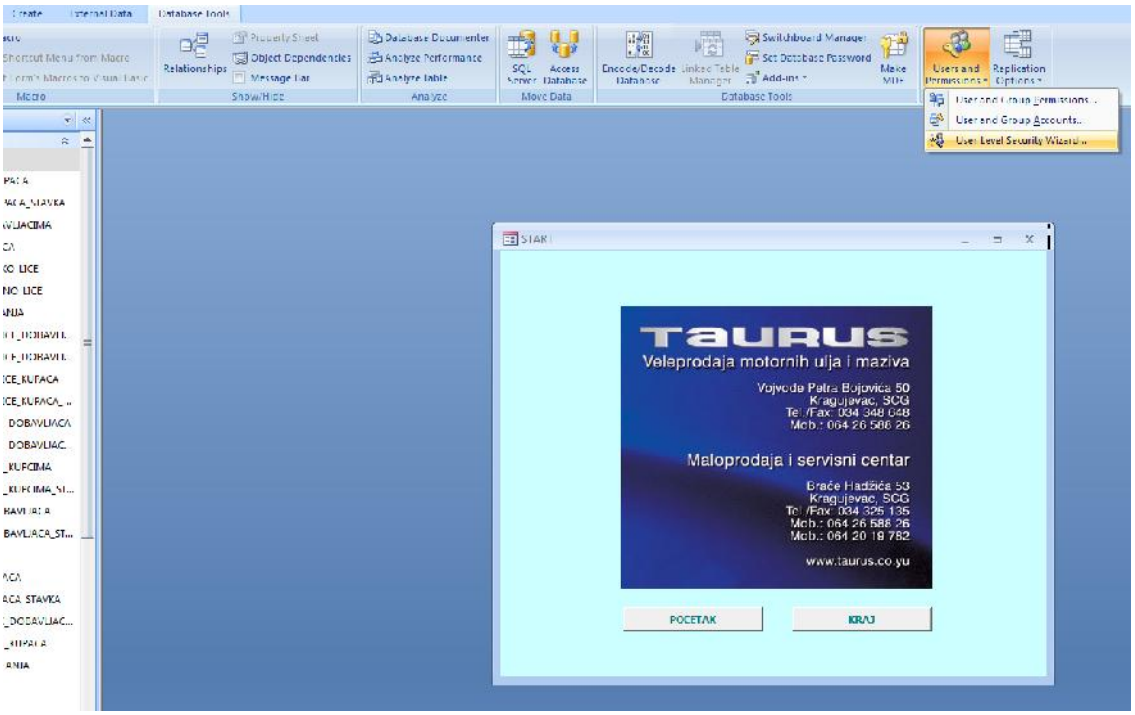
Slika 17 Message bar

4.2 Access User - level security

U narednom primeru ćemo pregledati Access User - level security, funkcija koja nam omogućavaju da se odredi nivo pristupa i da se odobri svaki pojedinačno korisnik baze podataka koji mogu pristupiti određenim podacima iz baze.

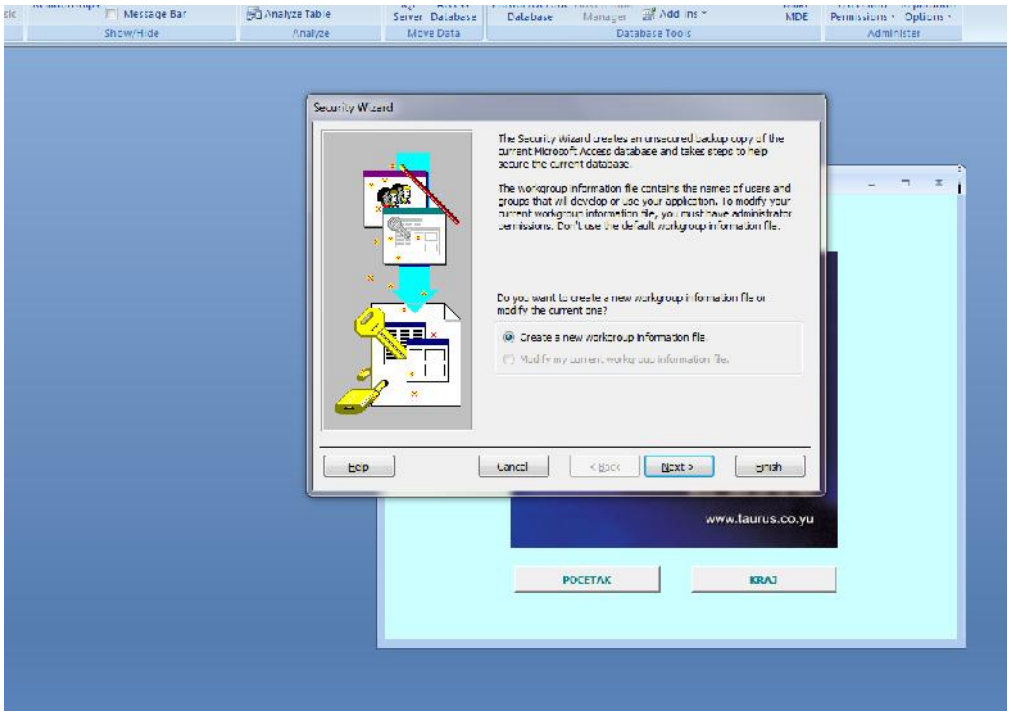
User - level security je moćan alat koji nam omogućava da kontrolišemo tipove podataka da bi korisnik pristupio (na primer, zabrana osoblja prodaje da gleda računovodstvene podatake) i akcije koje mogu da izvršavaju (npr. samo dozvoljavajuće odeljenje iz firme za promenu kadrovske evidencije). Važno je imati na umu da su ove funkcije kopija (sličnost) neke od funkcionalnosti više moćnih baza podataka, kao što su SQL Server i Oracle. Međutim, pristup je i dalje u osnovi jednog korisnika baze podataka.

Prvi korak je pokrenuti bazu podataka nakon toga sledeći korak je pokrenuti bezbednosni čarobnjak (Wizard), kao što je prikazano na slici. U meniju Database Tools, izaberemo opciju User and Permissions zatim Korisnički nivo bezbednosti čarobnjak.



Slika 18 user level security

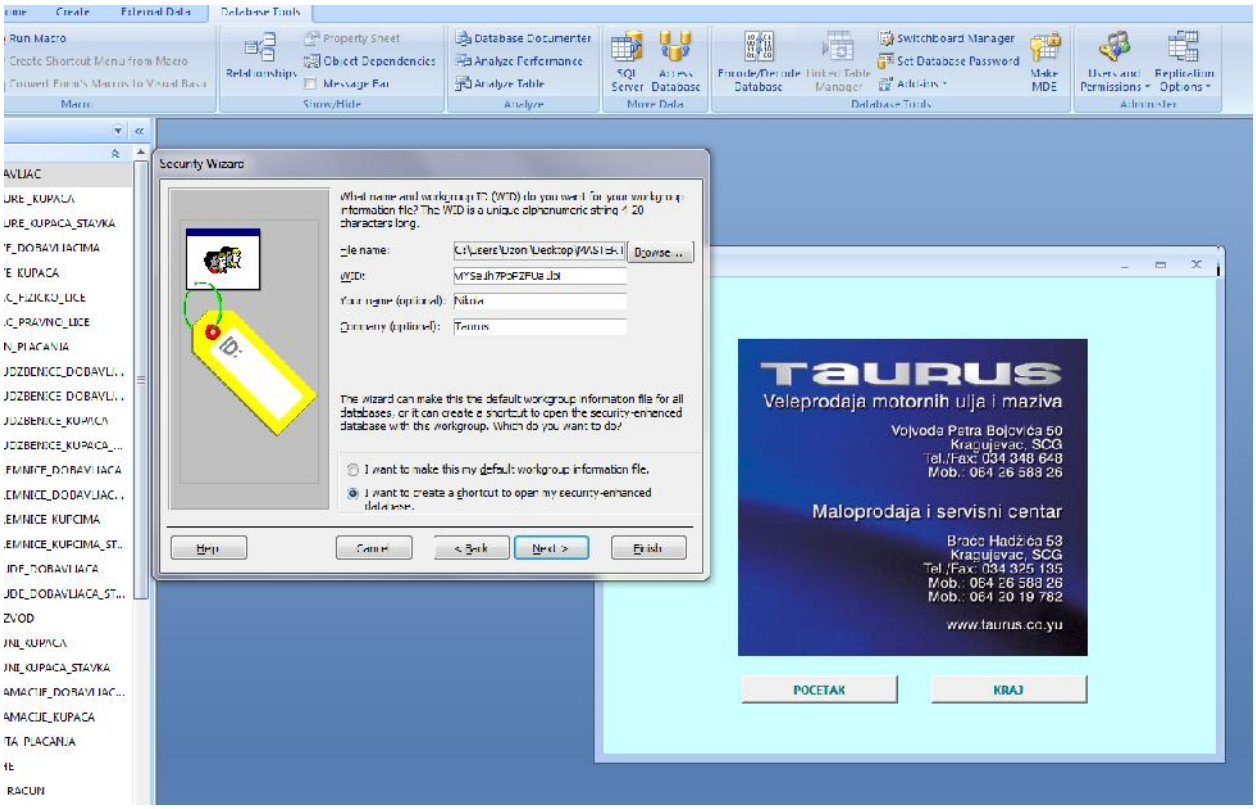
Nakon ovih koraka sledeči je prozor koji se otvara, i postavlja pitanje da li želimo da započnemo novu datoteku bezbednosti ili izmeniti postojeću. Mi ćemo pretpostaviti da želimo da pokrenemo novu, pa izaberemo "Kreiranje nove informacione datoteke radne grupe" i kliknite na Next.



Slika 19 Početak kreiranja

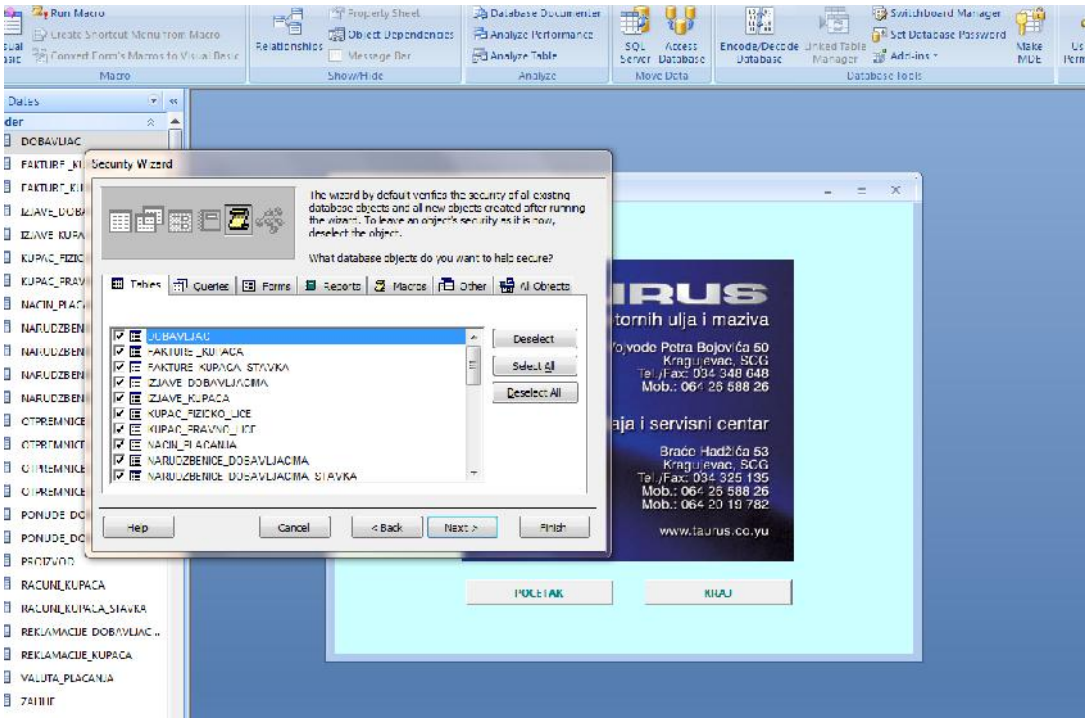
Sledeći od nas se traži da unesemo svoje ime i kompaniju. Ovaj korak je opcionalan, nakon toga se pojavljuje čudan string koji se zove Wid. Ovo je jedinstveni identifikator koji se dobio slučajnim odabirom računara i generalno ne treba menjati.

Nakon ovga sledeće što se od nas traži je da li želimo da naša bezbednosna podešavanja da primenimo samo na bazi podataka koju trenutno uređujemo ili da li želimo da dozvolimo da budu podrazumevane dozvole koje važe za sve baze podataka. Kada ovo popunimo, kliknemo na dugme Dalje.



Slika 20 Bezbednosna podešavanja

U sledećem koraku Wizard će zatim pitati koje objekte u našoj bazi podataka želimo da zaštitimo. Po defoltu (Podrazumevano), Access će obezbediti sve postojeće objekte odn. Tabele, upite, obrasce, izveštaje ili makroe, i sve nove objekte. Možemo da izaberemo objekte koje neželimo da budu zaštićeni, što znači da svi korisnici će imati pune dozvole za taj ne obezbeđeni objekat. Preporučljivo je da se ne zaobiđe zaštita za bilo koji objekat u bazi podataka. Mi ćemo pretpostaviti da želimo obezbedi kompletnu bazu podataka, tako da jednostavno pritisnemo dugme Next da bi smo nastavili dalje.

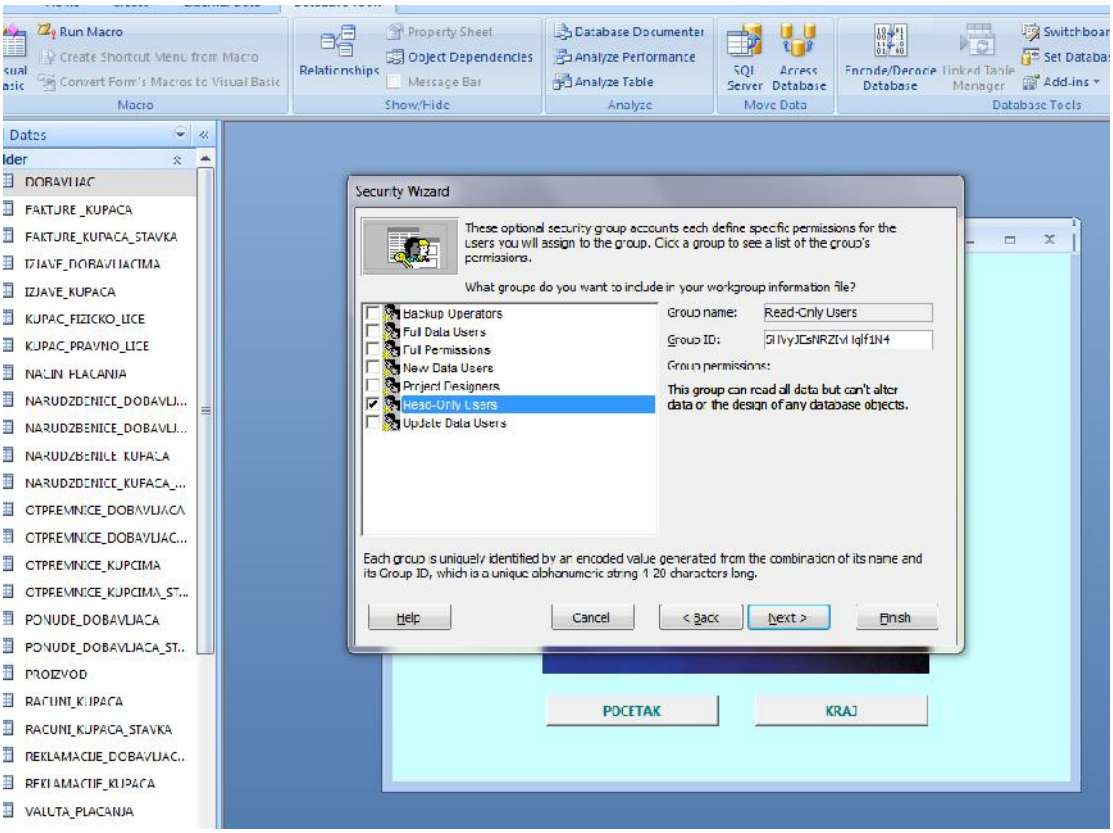


Slika 21 Šta zaštiti

U sledećem koraku Wizard nam omogućava da izaberemo koje grupe mogu da pristupe bazi podataka. Možemo da izaberemo svaku grupu da vidimo posebne dozvole primenjene na svaku grupu. Na primer :

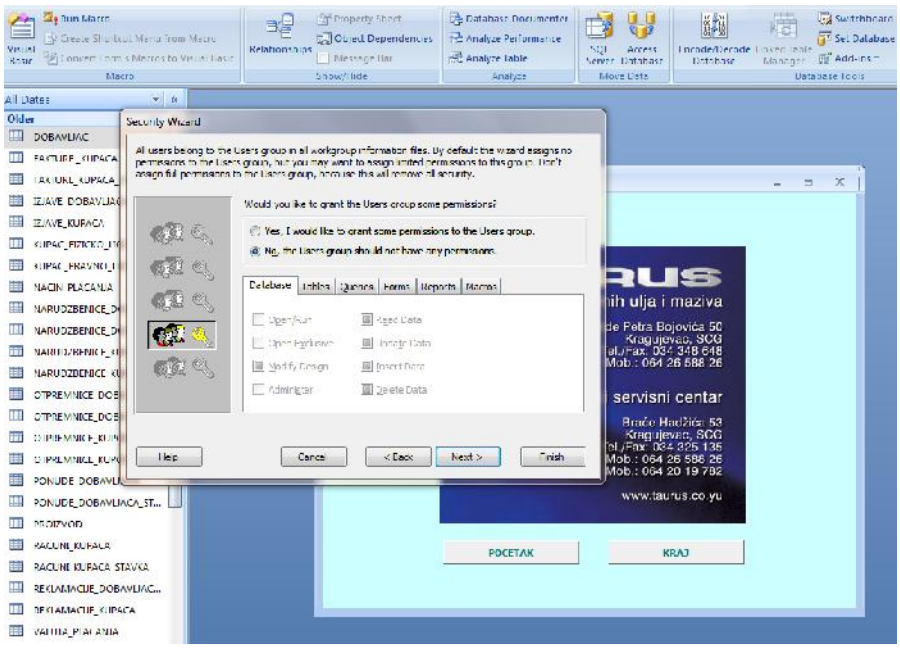
a. *Backup Operators* - grupa je u stanju da otvori bazu podataka radi pravljenja rezervnih kopija, ali ne mogu da čitaju objekte podataka
b. *Full Data Users* - grupa ima punu dozvolu za izmene podataka, ali ne mogu da menjaju dizajn svih objekata baze podataka
c. *Full Permissions* - ima punu dozvole za sve objekte baze podataka, ali ne može da dodeli dozvole drugom korisniku
d. *New Data Users* - može da čita i unosi podatake, ali ne mogu menjati dizajn bilo kog objekta baze podataka ili brisanje ili ažuriranje podataka
e. *Project Designers* - ima punu dozvolu da uređujete podatke i sve objekte, osim što ne mogu menjati tabele i relacije
f. *Read-Only Users* - ova grupa može da ima sve podatke, ali ne mogu da menjaju podatke ili dizajn bilo kog objekata baze podataka
g. *Update Data Users* - ova grupa može da čita i ažuriranje podataka, ali ne mogu da menjaju dizajn svih objekata baze podataka ili unese ili izbriše podatke.

Nakon ovog kratkog opisa mogućnosti koji nam se pružaju, mi ćemo izabrati Read - Only User i automacki nam se sa desne strane Group name popunjava sa Read-Only Users i Group ID koji računar dodaje. Nakon ovih zahteva klikom na dugme Next idemo dalje.



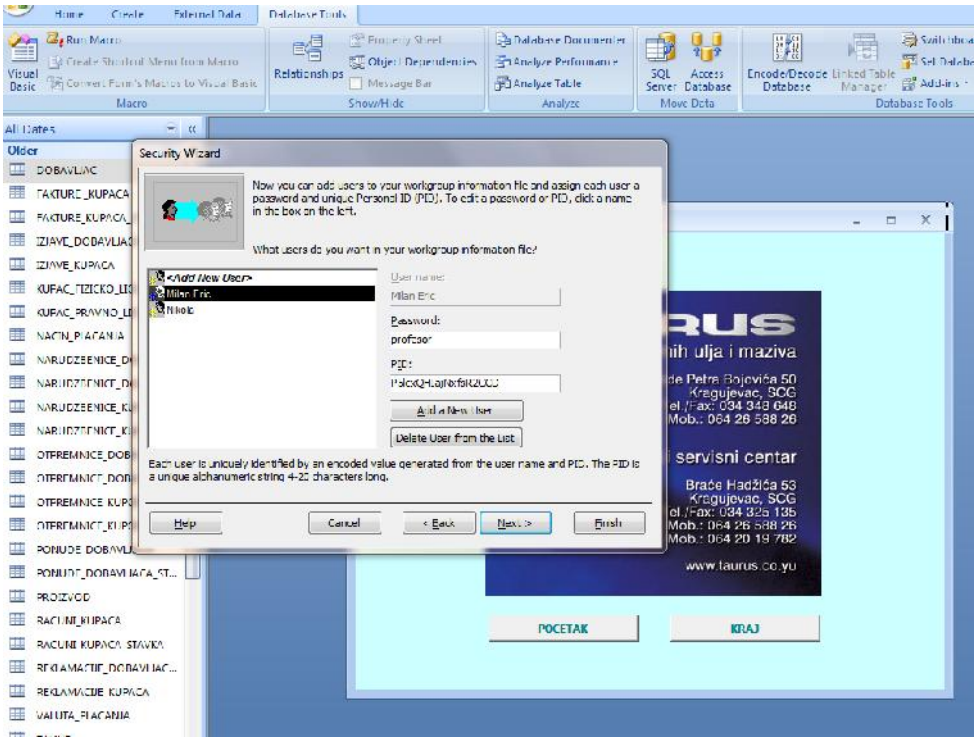
Slika 22 Grupe pristupa

Pored ovih raspoloživih grupa, Access kreira dve druge grupe, korisnike i administratora. Podrazumevano, svi korisnici baze podataka se dodaje u grupu korisnika. Oni korisnici koji su u grupi Admins imaju pune dozvole i jedini korisnici koji mogu da kreiraju dozvole i grupe. Za ovu vežbu," Ne, grupa korisnika ne bi trebalo da ima bilo kakve dozvole " opcija će biti izabrana.



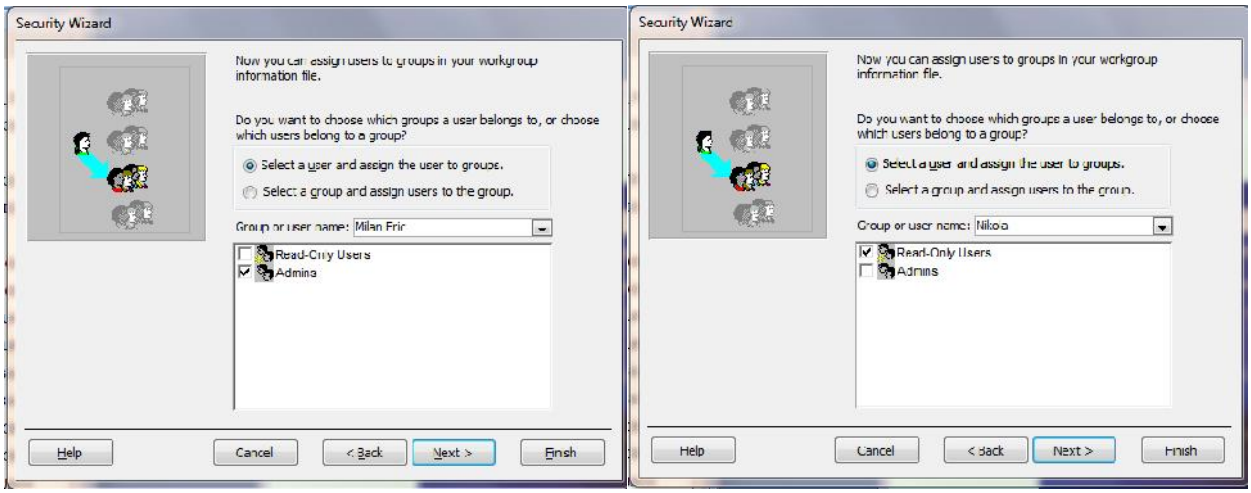
Slika 23 Grupe korisnika

Sledeći korak nam omogućava da kreiramo korisnike baze podataka. Možemo da kreiramo onoliko korisnika koliko god hoćemo tako što klikom na opciju Add a new user, dodajemo novog korisnika pod imenom i šifrom koju popunjavamo sa desne strane. Trebalo bi da dodelimo jedinstvenu, jaku lozinku za svakog korisnika baze podataka u ovom slučaju postavljamo Milan Erić sa šifrom Profesor, i Nikola sa šifrom Student. U principu, nikada ne bi trebalo da stvaramo zajedničke profile.



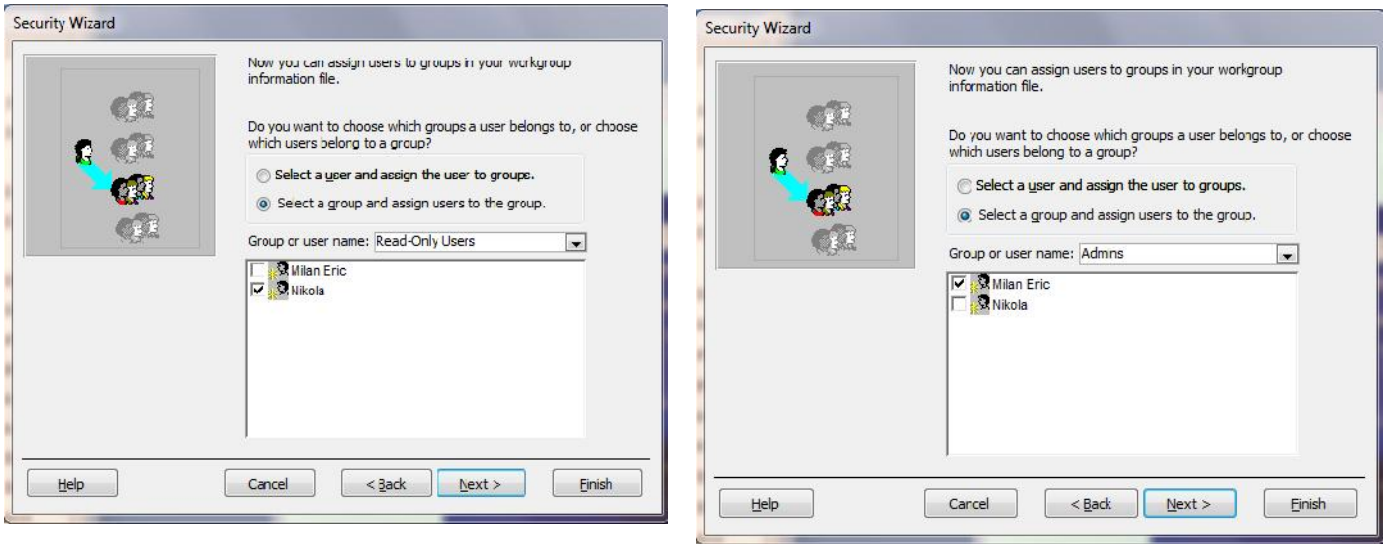
Slika 24 Korisnici baze

Sledeće on nas se traži da u prethodna dva koraka što smo popunuli sada samo konkretizujemo. Možemo izabrati svakog korisnika iz padajućeg menija, a zatim dodeliti jednu ili više grupa putem čekiranja. Tako da onoj grupi u kojoj postavimo korisnika imaće određene zabrane ili pogodnosti. Kao admina smo postavili Milana Erića, a kao Red-onley, Nikola.



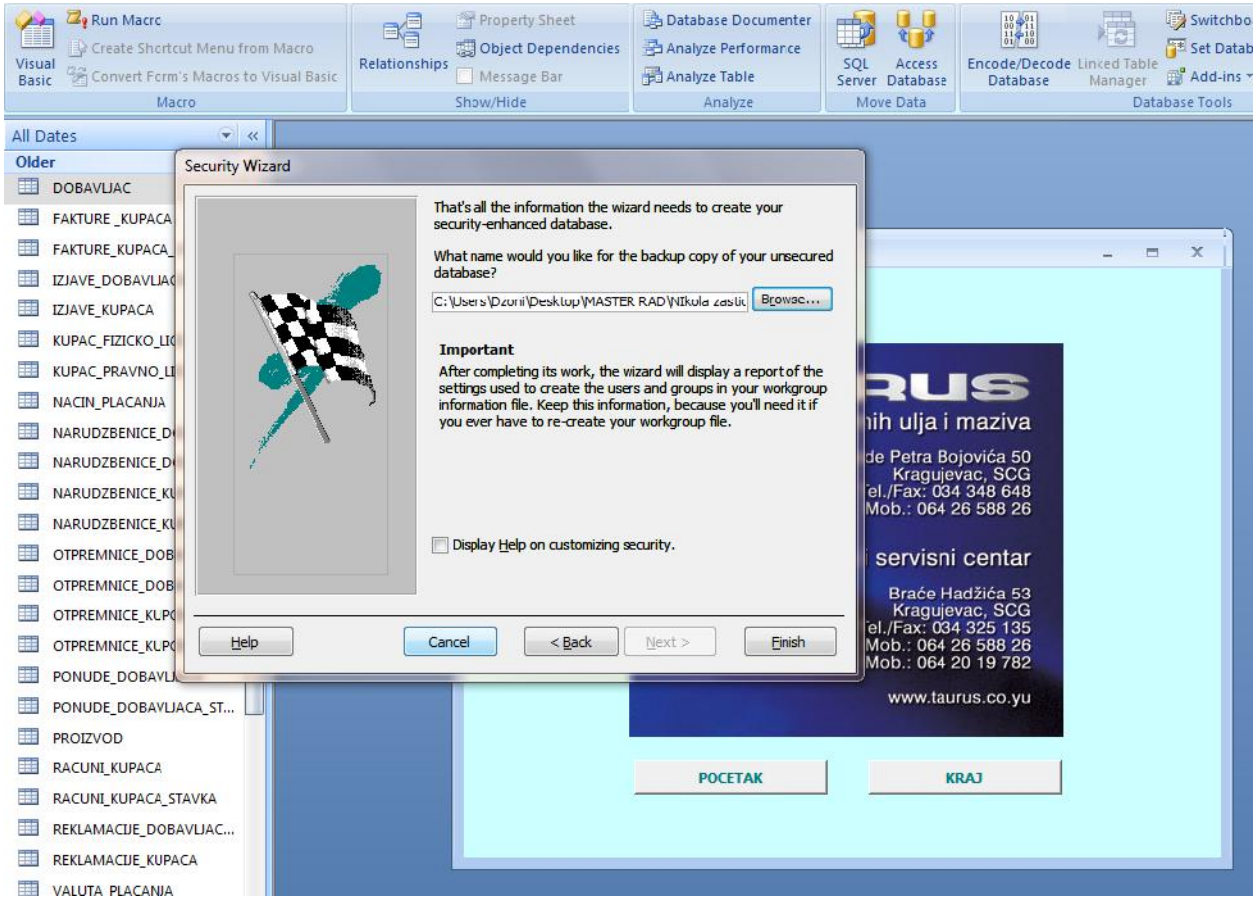
Slika 25 Izbor admina i korisnika

Ovo prethodno podešavanje je u funkciji kada čekiramo " Select user and assign user to groups ", međutim kada čekiramo " Select a group and assign users to the group ", onda na padajučem meniju imamo grupe koje smo prethodno napravili, a čekiramo korisnike grupe ko če kojoj grupi pripadati. (Slika 26) Nakon obih podešavanja kliknemo na Next.



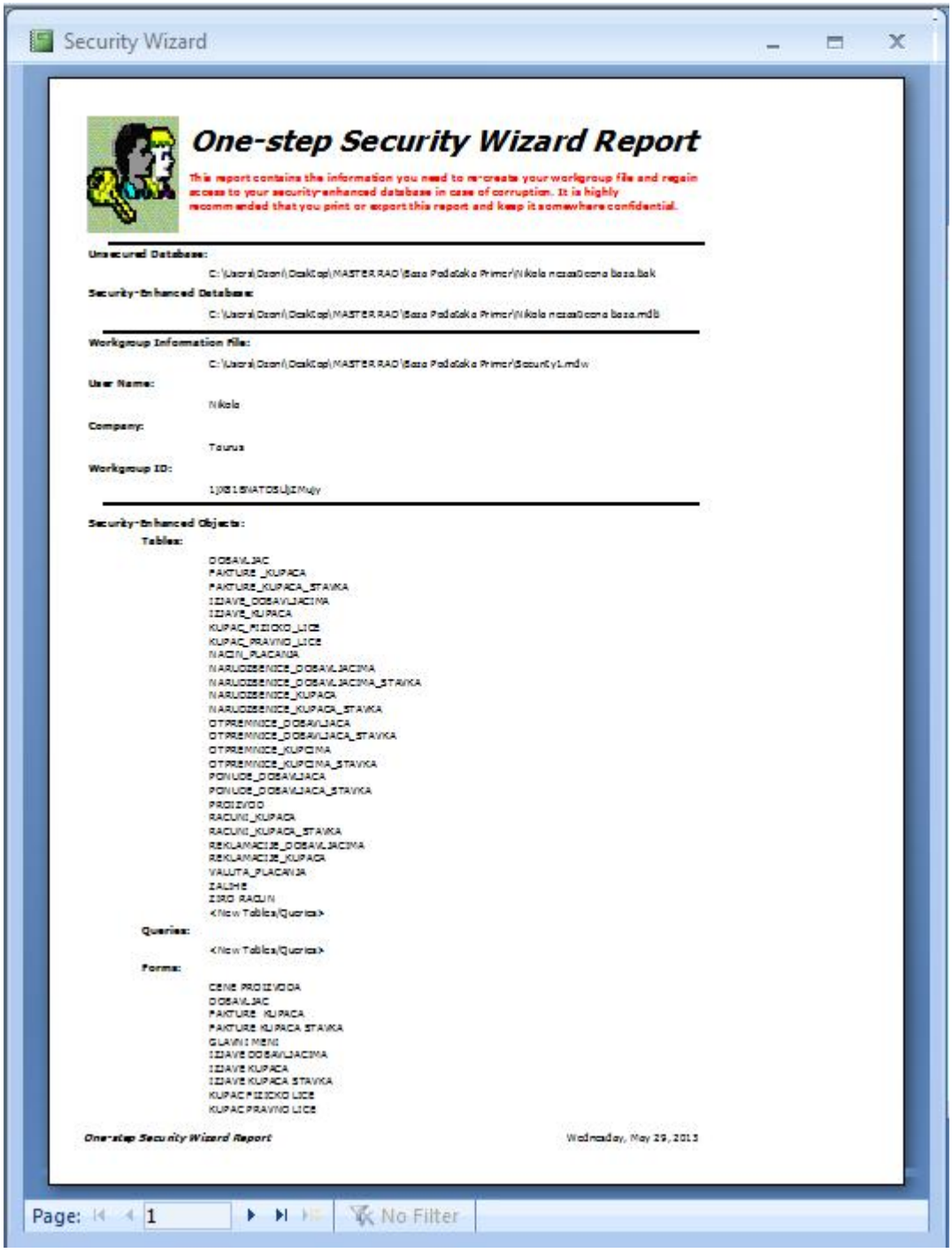
Slika 26 Izbor korisnika

I na kraju od nas se traži, da napravimo rezervnu kopiju podataka nešifrovane baze. Ovo je važno, jer nam omogućava da povratimo podatake ako zaboravimo korisničku lozinku. Rezervnu kopiju je dobro sačuvati na CD-u, a zatim držati CD na bezbednom mestu. Kada napravimo rezervni CD, treba da obrišete nešifrovane datoteku sa hard diska kako bi ga zaštitili od ostalih koji pristupaju našem računaru. Nakon ovih podešavanja uspešno smo implementirali korisnički nivo bezbednosti na bazi podataka. Poželjno je da se ove informacije sačuvaju pošto će nam biti potrebne u slučaju da moramo da ponovimo čitav proces, kako bi smo lakše ponovni process obradili, prikazano je na izveštaju ovih procesa.



Slika 27 Rezervna kopija

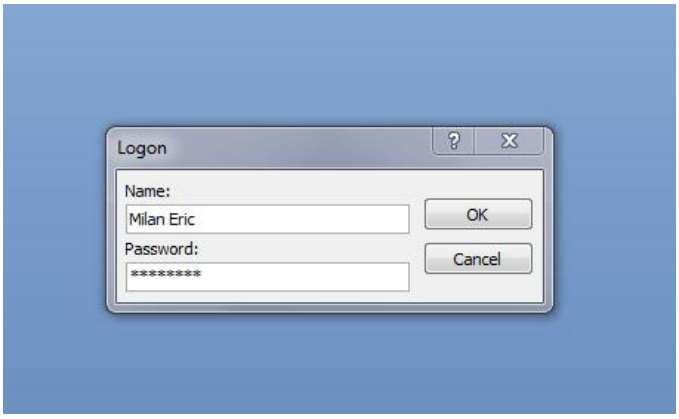
I na kraju kliknemo na dugme Finish, i pojaviće nam se One-step Security Wizard izveštaj, na kojem stoji gde nam se nalazi snimljena nešifrovana baza, zatim šifrovana baza, Ime korisnika, ime firme Workgroup ID, koji su objekti i forme zaštićene sa sve datumom kada je izvršena zaštita. Naredna slika 28 predstavlja izgled izveštaja.



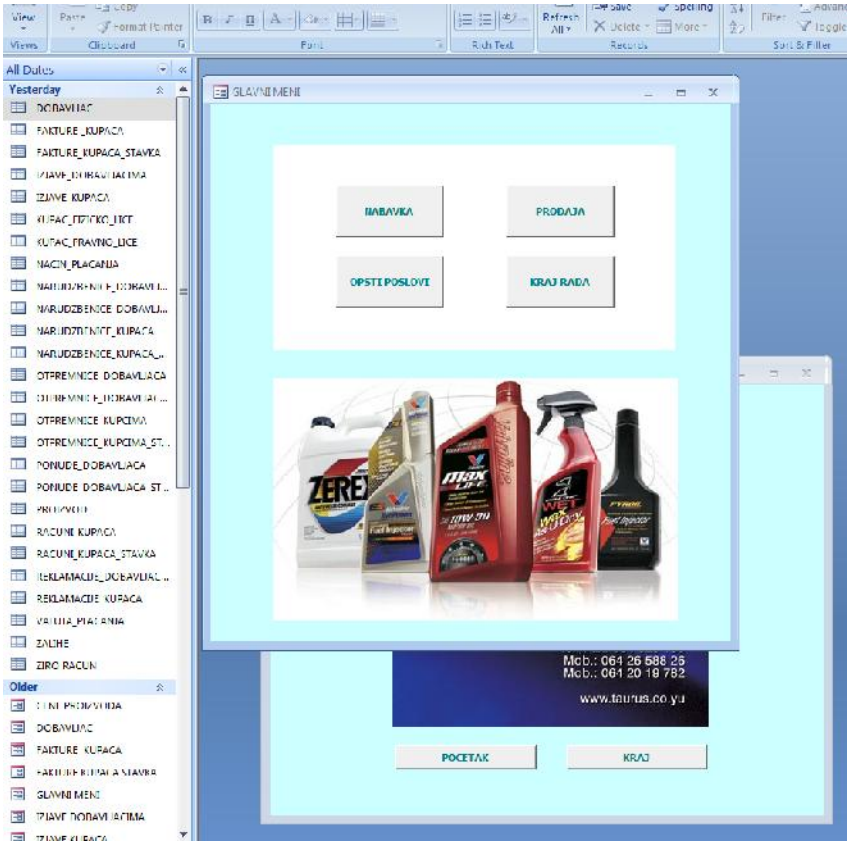
Slika 28 Izgled Izveštaja

Nakon ovih koraka, na slici 29 je prikazana slika sa ikonicom na kojoj se nalazi ključ koji nas asocira da je potreban user name i password kako bi smo pristupili bazi podataka, kada pokrenemo aplikaciju pojaviće nam se Logon koji je takđe prikazan na slici 30 i kada popunimo trežene atribute možemo pristupiti našoj bazi, ono što će nam se prikazati zavisi od toga kojoj grupi pripadamo koju smo u prethodnim koracima označili.

Slika 29 Ikonica



Slika 30 Login



Slika 31 Izgled radne površine nakon uspešno unešene šifre

5. Zaključak

Može se zključiti da današnji, savremeni informacioni sistemi ne mogu se zamisliti bez jedne baze podataka. Čitava današnja preduzeća, institucije, avio kompanije, banke, prosto ne mogu funkcionisati bez baze podataka, tako da je pitanje zaštite baze od velikog značaja.

U ovom radu su opisani zakoni na području Srbije koji se koriste, ISO standard za zaštitu informacija, osnovnih deset pretnji koji se javljaju i rešenja za njihovo otklanjanje. Zatim je opisana zaštita ključeva, čemu oni služe, koliko informacija oni obuhvataju, zatim njihov vek trajanja, podela na više ključeva koja postoji i rešenja za što sigurnije upravljanje i njihovu zaštitu. Nakon ovih osnovnih rešenja urađen je primer u Access-u na bazi podataka gde je prikazano kako se postavlja Login za konkretnu bazu i kako se Security warning aktivira i deaktivira.

Literatura :

[1] Pravna zaštita baze podataka Sinergija, http://www.singipedia.com/content/350-Pravna-zatita-baze-podataka

[2] Pavlović - Lažetić G:.**Osnove relacionih baza podataka**, Matematički fakultet, Beograd, 2000.

[3] Lazarević B : **Baze podataka** , FON Beograd , Beograd 2003

[4] ISO standard : http://www.mobes.rs/usluge/iso-27001.html

[5] Autorska agencija za Srbiju Intelektualna svojina : http://autorskaagencija.com/srp/pitanja/?conid=21

[6] BSA Global Software Piracy: http://globalstudy.bsa.org/2011/index.html

[7] Top deset pretnji na bazu podataka : http://www.imperva.com/docs/WP_TopTen_Database_Threats.pdf

[8] Pleskonjić D., Maček, N., Đorđević B., Carić M., Sigurnost računarski sistema i mreža, Mikro knjiga 2007.

[8] Microsoft ovlašćeni sajt : http://office.microsoft.com/en-us/access/