Poboljšanje Sigurnosti Sistema Putem Windows Registry Baze

by m4rk0

1. UVOD

Ovaj tutorijal je vlasnistvo sajta http://tutoriali.org/ i njegovog autora. Autor ovog tutorijala je m4rk0. Objavljivanje ovog tutorijala je moguce iskljucivo u nepromenjenoj formi i uz obavezu navodjenja izvora i autora tutorijala.
Da biste sto bolje razumeli ovaj tutorijal, preporucujem vam da procitate moj prethodni tutorijal o redzistriju. Sa informacijama koje budete prikupili, razumecete ovaj tutorijal sasvim dovoljno za pocetak. Izabrao sam (ponovo) redzistri kao tematiku za moj tut, iz prostog razloga sto je po meni redzistri najvaznija "komponenta" windows operativnog sistema. U ovom tutorijalu cu objasniti znacaj redzistrija u pogledu (poboljsanja) sigurnosti windoze. Moc i brojnost opcija u redzistriju impresionirace vas, stoga dobro otvorite oci, zadrzite dah i krenite sa citanjem :>

1.1 Lista za kontrolu pristupa (Access control list a.k.a ACL)

Prva stavka koju cu objasniti je **ACL** tj **access control list**. Sam prevod na srpski vam objasnjava sta je to ustvari. Znaci to je komponenta windows sigurnosti koja vrsi separaciju dozvola na racunaru tj. bukvalno receno - kontrolise pristupe razlicitih korisnika windoze. To je jedna lista korisnika i dozvola koje isti imaju na racunaru. ACL-u se pristupa tako sto udjemo u redzistri, pronadjemo zeljeni kljuc sa access control listom, i idemo desni klik -> permissions. Admin moze dodeljivati nove dozvole ili oduzimati postojece: pokretanje procesa, fajlova, programa. Takav oblik podesavanja je preporucen iskljucivo ukoliko postoji ogromna potreba za istim i ukoliko je to znaci jedino resenje za resavanje nekog "problema". Pocetnicima, ova vrsta podesavanja verovatno nije ni potrebna, ali naprednim korisnicima je itekako potrebna jer defultni permissioni u okviru windoze su veoma oskudno podeseni. Ovo je samo osnova o ACL cisto da vam zagolicam mastu, a o potpunoj administraciji koja se moze izvesti preko ove security komponente cu vam pricati u nastavku tutorijala. ACL ce se "provlaciti" gotovo kroz ceo tutorijal.

1.2 Group Policy Object a.k.a GPO

Bitno je istaci da postoje dva metoda podesavanja dozvola. Prvi nacin je preko redzistrija i to direkto preko ACL, a drugi nacin je pravljenje sigurnosnih timplejtova (security templates) koji u sebi sadrze sve lepo ispodesavane sigurnosne dozvole (security permissions) i nakon pravljenja takvog jednog timplejt, jednostavno rucno ucitate taj timplejt i imate sve ispodesavano kao na tanjiru. Oni koji znaju sta je pojam "template" na pr u web dizajnu, shvatice i sustinu timplejta kod windoze (molim samo da ne budete bukvalisti :>). U prenosnom znacenju template je shablon sa svim potrebnim podesavanjima koji, takodje, moze predstavljati odlicnu osnovu za dalja (napredna) podesavanja. Elem, gorespomenute timplejte podesavamo preko **Grop Policy Object** (u daljem tekstu **GPO**). Do Grop Policy editora stizemo tako sto u run-u kucamo **gpedit.msc** . U okviru njega mozemo izvrsiti podesavanja registrja, NTFS sigurnosti, software instalacije, logon/logoff skripti, redirekcije foldera i podesavanja Internet Explorer-a. Princip rada je sledeci: Mi kreiramo GPO i onda importujemo sigurnosne timplejtove u taj GPO da bismo kreirali security policy ("sigurnosnu politiku") za nasu mrezu, sistem...Windows zatim automatski dodeljuje komjuteru i korisniku dozvole zadate unutar sigurnosnih timplejtova, ukoliko je taj GPO "pristupacan".

2. Podešavanje sigurnosti putem ključeva

2.1 Osnovna podešavanja dozvola putem ključeva

Ako imate admin prava na OS-u, mozete podesavati dozvole za pojedinacne korisnike ili citave grupe i sve to naravno preko ACL-a. Postupak je sledeci: Za pocetak normalno udjite u redzistri i pronadjite kljuc u okviru koga zelite da menjate dozvole i desni klik -> **permissions** i otvori ce vam se nov prozor sa listom korisnika/grupa a ispod se nalaze dozvole selektovanog korisnika/grupe:

- **Full Control** - Omogucava korisniku ili grupi korisnika potpunu administraciju nad kljucem. Znaci korisnik moze da otvara, edituje i preuzima vlasnistvo nad selektovanim kljucem.

- **Read** - Omogucava korisniku ili grupi korisnika iskljucivo da "citaju" kljuc (ali ne mogu da sacuvaju promene koje su napravljene u okviru kljuca). Znaci to je read-only dozvola.

- **Special Permissions** - Omogucava korisniku ili grupi korisnika posebne kombinacije dozvola. Do ove opcije dolazi se preko dugmeta advanced u okviru ACL-a.

Cesto se desava da su check polja zamagljena i da ne moze da se cekiraju dozvole za selektovanog korisnika ili grupu. To znaci da ta opcija trenutno nije dozvoljena. To se desava iz prostog razloga sto taj kljuc nasledjuje dozvole od maticnog kljuca. Postoji nacin zastite kljuca od "nasledjivanja dozvola" i o tome cu pricati u delu tutorijala pod nazivom "special permissions (assigning)"

2.2 Kontrolisanje korisnika putem ACL-a

Sto se tice kontrole dozvola korisnika putem ACL-a, ukratko cu vam objasniti nacine dodavanja i skidanja korisnika sa ACL. **Dodavanje** vrsimo tako sto u redzistriju pronadjemo kljuc za koji zelimo da oznacimo dozvole koje ce korisnici ili grupe korisnika imati. Zatim idemo desni klik pa **permissions** i klik na **add**. U novootvorenom prozoru kliknemo na location, selektujemo komp, domain ili organizacijsku jedinicu sa koje zelimo da dodamo korisnike na ACL. Ovde se moze desiti da ne znate tacan naziv ili ceo naziv korisnika ili grupe koje dodajete ACL-u. Ali postoji resenje za to. Jednostavno u okviru prozora kod koga dodajete usere kliknite na **advanced** pa na **Find Now**. Pojavice vam se kompletna lista korisnika i grupa i jednostavno dodajte ACL-u korisnike ili grupe koje zelite. Na kraju u **permissions for..** prozoru podesite dozvole za dodate korisnike i grupe korisnika. Dodavanje korisnika u ACL je veoma korisno za neke stvari tipa pristup vasem redzistriju sa udaljenih mesta ako je to potrebno. Na pr zadesiti se u tunguziji, podigli ste server kuci i zelite da iz tunguzije da izmenite neke stavke u redzistriju sto je hitnije moguce a ne mozete da dodjete do kompa jer vam je hiljadama kilometara udaljen. Jednostavno mozete pristupiti kompu sa vaseg na pr laptopa iako ste kilometrima daleko i izvrsiti potrebne zahvate. To je samo jedan banalni primer i u praksi ima dosta koristi od dodavanja korisnika na ACL, Medjutim postoji i losa strana dodavanja korisnika na ACL pogotovo ukoliko neko nema velikih iskustava sa tim ili jednostavno napravi slucajnu gresku u koracima i na taj nacin napravi veliku rupu u operativnom sitemu, tj. vetil kroz koji informacije mogu da izlecu sa vaseg kompa. Kada zelimo maknuti nekog od korisnika sa ACL-a, to mozemo vrlo lako uraditi. U redzistriju pronadjemo kljuc za koji zelimo da oznacimo dozvole koje ce korisnici ili grupe korisnika imati. Zatim idemo desni klik pa **permission**s i klik na **Remove**. Simple as that :> Ipak i ovde moramo obratiti paznju na odredjene stvari. Sve sto vidimo u okviru ACL (a tu se nalazi po defaultu) predstavlja nesto najminimalnije, tek toliko da korisnici mogu startuju i koriste windozu. Ukoliko uklonite korisnike ili korisnicke grupe iz kljuca, ti korisnici nece

biti u stanju da "citaju" kljuceve sto dalje implicira na to da ti isti korisnici nece biti u stanju da "upravljaju" windozom i njegovim aplikacijama. A zamislite onda sta bi se tek desilo kada bi uklonili Administrators group iz kljuca :> Ladno ne biste mogli ni vi sami da upravljate vasim OS-om. A ako uklanjate pojedinacne korisnike, to i nije tako "opasno", jer ni sam windows ne pruza dozvole individualnim korisnicima i ne treba da uklanjate pojedincane korisnike iz ACL-a, jer na taj nacin ih sprecavate da pristupaju njihovim sopstvenim podesavanjima, a koji naravno treba da imaju punu kontrolu.

2.3 Specijalne dozvole (dodela)

Ukoliko zelimo da izvrsimo podesavanja dozvola koja su znatno detaljnija od full control i read dozvola, to mozemo izvrsiti preko **Special Permissions** opcije (dugme **Advanced** u okviru ACL-a). U okviru ove opcije mozete vrsiti znatno detaljnija podesavanja tipa "citanje", "pisanje" kljuceva, editovanje podkljuceva..Kada ste izvrsili podesavanja pojavice se apply padajuca lista sa sledecim opcijama:

- **This key only** - Primenjuje podesene dozvole zamo na selektovani kljuc
- **This key and subkeys** - Primenjuje podesene dozvole na selektovani kljuc i sve podkljuceve u okviru tog kljuca.
- **Subkeys only** - Primenjuje podesene dozvole na sve podkljuceve u okviru selektovanog kljuca, ali ne i na sam kljuc.

U permission listi imacete opcije **allow** (dozvoliti) i **deny** (odbiti) za sledece dozvole:

- **Full Control** - Sva moguca podesavanja
- **Query Value** - Citanje vrednosti u okviru kljuca
- **Set Value** - Postavljanje vrednosti u okviru kljuca
- **Create Subkey** - Kreiranje podkljuca u okviru kljuca
- **Enumerate Subkeys** - Identifikacija podkljuca u okviru kljuca
- **Notify** - Primanje obavestenja o dogadjajima od strane kljuca
- **Create Link** - Kreiranje simbolicnih linkova unutar kljuca
- **Delete** - Brisanje kljuca ili njegove vrednosti
- **Write DAC** - Pisanje kljucevog DAC-a (discretionary access control list)
- **Write Owner** - Izmena vlasnika kljuca
- **Read Control** - Citanje DAC-a

Pominjao sam "nasledjivanje" dozvole od maticnog kljuca a da malo detaljnije objasnim to. Ukoliko je nasledjivanje omoguceno, podkljucevi nasledjuju dozvole njihovih maticnih kljuceva. Drugim recima, ukoliko kljuc omogucava grupi punu kontrolu, svi njegovi podkljucevi takodje omogucavaju grupi punu kontrolu. Ukoliko su polja za cekiranje dozvola u okviru ACL-a za selektovanu grupu korisnika zamagljena, to znaci da ne mozete menjati nasledjivacke dozvole kljuca. Sto se tice podesavanja nasledstva kod kljuceva, mozemo na pr da zastitimo podkljuceve od nasledstva dozvola od strane maticnih kljuceva i to u okviru **Advanced Security Settings For..** prozoru, gde decekiramo **Inheritable Permissions**. Takodje mozemo da izvrsimo i zamenu ACL podkljuceva u uokviru kljuca, resetovanjem kompletne grane kako bi odgovarao kljucevom ACL-u a to se postize tako sto cekirate opciju: **Replace Permissions Entires On All Child Objects**...

2.4 Standardne Dozvole (mapiranje)

Da bismo razumeli defaultne dozvole, neophodno je razlikovati 3 grupe u okviru windoze, a to su: Users, Power Users i Administrators. Svaka od ove tri grupe ima poseban nivo dozvola.

- **Users** - Ova grupa je najsigurnija jer po defaultu toj grupi nije dozvoljeno da izmenjuje podatke u okviru OS-a i druga podesavanja. Oni mogu cackati iskljucivo programe sertifikovane od strane windoze , koje administrator zadaju njihovim kompovima. Ova grupa moze da vrsi potpunu kontrolu svojih profila ukljucujuci i HCKU. Napredni korisnici cesto ne vrse kreiranje ovakvih grupa jer korisnici uglavnom i ne pokrecu legalne aplikacije, pa se admini stoga ipak okrecu pravljenjem sigurnosnih timplejtova.

- **Power users** - Ova grupa korisnika u odnosu na "Users" grupu, moze pokretati i programe koji nisusertifikovani od strane windowsa. Po defaultim podesavanjima, power users grupi je omoguceno da vrsi veliki broj podesavanja u okviru OS i aplikacija. Ukoliko imate legalne aplikacije koje korisnici koji pripadaju grupi Users ne mogu da pokrenu, a ne zelite da primenjujete sigurnosne timplejtove, jednostavno prebacite korisnike u Power Users grupu i korisnici ce moci da pokrecu te aplikacije. Korisnici ove grupe mogu da instaliraju vecinu aplikacija, ali ne mogu menjati sistemske fajlove i instalirati servise. Power Users se prema dozvolama nalaze izmedju Users i Administrator grupe i naravno, na kraju krajeva, korisnici ove grupe ne mogu sebe dodavati u Administrators grupu.

- **Administrators** - Ova grupa moze da vrsi sva moguca podesavanja i ima potpunu kontrolu nad sistemom. Oni mogu vrsiti sva podesavanja u redzistriju - preuzimati vlasnistvo nad kljucevima i menjati ACL. Ni u kom slucaju nemojte dodavati neke druge korisnike u Administrator grupu, jer to je isto kako kad bi nekome dali kljuceve od vaseg stana ili kola. Naravno, niko nece vrsiti podesavanja i upravljanja nego vi sami.

3. Manipulacija sigurnosnim pristupima

3.1 Kontrola pristupa redžistriju

Nadgledanje desavanja u okviru redzistrija naziva se **auditing**. (pregled). Auditing se sastoji iz tri koraka.

- Prvo treba da ukljucimo **Audit Policy**. To se moze uraditi preko GP editora. Znaci otici u **control panel** (classic view) -> **administrative tools** -> **local security policy** nakon toga kliknuti na **Audit Policy** (sa leve strane prozora). U desnom delu prozora dvoklik na **Audit Object Access** i chekirati **Success** i **Failure**. Na taj nacin je Audit Policy ukljucen.

- Nakon toga treba u redzistriju izvrsiti pregled individualnih kljuceva i to na sledeci nacin: pronadjite zeljeni kljuc i **desni klik** na njega -> **permissions** -> **advanced** -> tab **Auditing** -> **add** -> **location** -> selektovati zeljeni komp, domen ili organizaciju u okviru cijih korisnika i korisnickih grupa zelimo da vrsimo pregled.

- Zatim u polju **Enter the object name**.. uneti ime korisnika ili korisnicke koju zelimo dodati audit listi i onda OK. U prozoru **auditing entry for**.. u acces listi cekirati i **successful** i **failed** za one aktivnosti za koje zelite da vrsite pregled uspesnih i neuspesnih pokusaja. Posle ukljucivanja **Audit Policy**, treba to sve lepo proveriti preko **Event Viewera**.

3.2 Zaštita redžistrija od lokalnog pristupa

Postavlja se pitanje, da li mozemo U POTPUNOSTI zastititi redzistri tako da korisnik ne moze da pristupi njemu. Odgovor je NIKAKO :> , iz prostog razlogasto redzistri sadrzi podesavanja koje korisnik mora da bude u stanju da "procita" kako bi win iole normalno radio. A uz sve to korisnici moraju imati punu kontrolu nad svojim profilima. Znaci jednostavno ne mozete potpuno spreciti pristup redzistriju, ali mozete napraviti kompromis - ograniciti dozvole korisnicima. Ukoliko ste admin mozete donekle onemoguciti pristup redzistriju ukljucivanjem opcije Prevent Access to registry editing tools. Ako ste to ukljucili, onda ce se u slucaju da neki korisnik pokusa da pristupi regeditu, videce error: **registry editing has disabled by administrator**. Tu sad postoji problem. Na taj nacin se onemogucava pristup redzistriju preko M$ regedita, ali ne i preko nekih alternativnih reg editora. Drugi nacin je upotrebom **Software Restriction Policies**, ali cak ni na taj nacin ne mozemo zastititi redzistri da korisnik ne moze da mu pristupi.

3.3 Sprečavanje remote načina pristupa redžistriju

U ovom pasusu iznad sam pricao o lokalnom pristupu redzistriju (tj zastiti od istog). Sada cu sve to objasniti samo o "daljinskom" (remote) pristupu redzistriju. Na windozi, korisnici lokalnih administrator i backup operator grupa mogu da pristupaju redzistriju daljinskim putem. Posto je **Domain Admins grupa** clan svake lokalne Aministrator grupe, svi **domain administratori** mogu da pristupe redzistriju svakog kompa koji je ukljucen u taj domain. Winodws XP mnogo vise zadaje restrikcija za pristup redzistrijuu odnosu na prethodne verzije. Da bi se omogucilo nekoj grupi da pristupa redzistriju na daljinu neophodno je u glavnoj jedinici kreirati administratorsku grupu za svaku organizacijsku jedinicu. To se radi tako sto se ta grupa doda u ACL kljuca:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

4. Sigiurnosni timplejtovi - security templates

4.1 Manipulisanje Sigurnosnim timplejtovima

Sigurnosni timplejtovi (**security templates**) se koriste za pravljenje security policy za vas komp ili mrezu. Pravljenje sigurnosnih timplejtova je znatno bolje i efikasnije od prethodno pomenutih tehnika posto sigurnosni timplejtovi omogucavaju da se izvrse konkretnija i komplikovanija sigurnosna podesavanja za veliki broj racunara koja znatno olaksavaju i ubrzavaju posao u odnosu na druga sigurnosna podesavanja. Kod njihovog pravljenja upotrebljavamo razlicite alatke. Prvo koristimo sigurnosne timplejtove za kreiranje i editovanje timplejtova. Zati koristimo **Security Configuration And Analysis** i **Group Policy** konzolu da bi smo primenili timplejtove. Preko timplejtova mozemo podesavati sledece kategorije:

- **Account policies** - Password Policy, Account Lockout Policy i Kerberos Policy
- **Local Policies** - Audit Policy, User Rights Assignment i Security Options
- **Event Log** - Application, System i Security Event Log podesavanja
- **Restricted Groups** - Clanstvo security-sensitive grupa
- **System Services** - Startup i dozvole za system servise
- **Registry** - Dozvole za for registry kljuceve
- **File system** - Dozvole za fajlove i foldere

Sigurnosni timplejtovi su najobicnniji **.inf** fajlovi. Znaci **txt** fajlovi sa inf extenzijom i veoma lice na **.ini** fajlove, sto znaci da ih opusteno mozete kopirati i editovati po potrebi. Postoji mogucnost i da sami napravite svoj security template "od nule" tj. "from scratch", ali to nije preporucljivo posto ima puno posla a rizik je preveliki, tako da je bolje da editujete vec postojece predefinisane windowsove sigurnosne timplejte. Bitno je napomenuti da samo clanovi Administratorske grupe imaju mogucnost da menjaju defaultni security template folder - **%SystemRoot%\Security\Templates** .

4.2 Kreiranje MMC

Za rad sa sigurnosnim timplejtovima najbolje je koristiti **MMC** (**microsoft managment console**). Princip je sledeci: u run-u ukucajte mmc i sibnite enter i u novootvorenom prozoru idite na **file** - **add/remove snap-in** -> **add** -> selektujte **Securiry Templates** i onda **add**. Nakon toga selektujte **Security Configuration And Analysis** i opet **Add**. Zatim zatvorite prozor i OK. Sacuvajte podesavanja - **File** -> **Save** i sacuvajte na pr kao **m4rk0Temps.msc** i fajl ce po defaultu biti sacuvan u **Administrative Tools folderu**. Da bi ga na brzaka startovali, idemo start -> all programs ->administrative tools -> m4rk0Temps ili kako ste ga vec nazvali.

4.3 Predefinisani Timplejtovi - Predefined Templates

U windozi vec postoji nekoliko predefinisanih sigurnosnih timplejtova. Znaci nemate potrebu da pravite nove timplejtove, vec jednostavno da editujete postojece po potrebi. Predefinisani timplejtovi se nalaze na sledecoj lokaciji: **%SystemRoot%\Security\Templates** i to sledeci:

- **Default security (security.inf)** - Defaultna sigurnosna podesavanja postavljena pri instaliranju wina. Takodje sadrzi i sistemske i redzistry dozvole. Posto ovaj timplejt sadrzi defaultna sigurnosna podesavanja, u slucaju da nesto zeznete, ovaj timplejt ce vam omoguciti da vratite sistem na originalna windows sigurnisna podesavanja, tako sto cete ovaj timplejt ucitati preko Security And AnalYsis konzole, a ne preko Group Policy.

- **Compatible (Compatws.inf)** - Ovaj timplejt "olaksava" restrikcije koje su zadate Users grupi dovoljno da mogu da pokrecu legalne aplikacije. Na ovaj nacin se zadaje mogucnost da se korisnici prebacuju iz Users grupe u Pawer Users grupu ili Administrator grupu. Ovaj timplejt takodje omogucava dozvole koje user grupe imaju na sistemskim fajlovima i aplikacijama tako da oni mogu da mogu da upravljaju aplikacijama i fajlovima koji nisu sertifikovani od strane winodwsa. Preko ovog timplejta administratori pomeraju korisnike iz Power users grupe u User grupu.

- **DC Security (DC Secutity.inf)** - Ovaj timplejt je kreiran kada je server pokrenut od strane domain kontrolera. Utice na fajlove, redistri i sistemske servise.

- **Secure (Secure*.inf)** - Ovaj timplejt izvrsava najfinija podesavanja. Na pr Securedc.inf je za domain kontrolere, a Securews.inf je za workstatione. Primenjuje snazne sifre, audit podesavanja.. Ogranicava korisnike LAN Manager i NTLM konfigurisanjem windowsa da salje samo NTLM v2 odgovore i konfigurisanjem servera da odbijaju LAN Manager odgovore. I na kraju, ovajtimplejt ogranicava anonymous korisnike sprecavajuici od enumeracije account naziva, enumeracije shareova, i prevodjenja SID-ov.

- **Highly Secure (Hisec*.inf)** - Ovaj timplejt predstavlja skup prethodnih timplejtova i zadaje jos veca ogranicenja. Hisecdc.inf je za domain kontrolere i Hisecws.inf je za workstatione. Ovaj timplejt na pr postavljanivo enkripcije i upisivanje u windows neophodno za autentifikaciju i za prenos podataka preko sigurnosnih kanala i to zashteva snaznu enkripcijui upisivanje. Na kraju ovaj timplejt uklanja sve korisnike iz Power Users grupa i proverava da li su iskljucivo Domain Admins grupe i lokal Administraori su korisnici lokal Admnistrator grupe.

- **System root security (Rootsec.inf)** - Ovaj timplejt opisuje root dozvole za win fajl sistem. Sadrzi dozvole koji nisu vezani za redzistri. Prihvata dozvole za root %SystemDrive% -a.

- **No Terminal Server user SID (Notssid.inf)** - Ovaj timplejt uklanja nepotrebne Terminal Server SID-ove sa file sistem i redzistri kada jepokrenut Terminal Server u aplikacijski kompatibilnom modu. Ako je to moguce,pokrenite Terminal Server u full sigurnosnom modu (u modu u kome se Terminal Server uopste ne koristi).

4.4 Kreirajte sopstveni timplejt

Postoji mogucnost da napravite sopstveni timplejt iako nije bas preporucljivo. To se radi na sledeci nacin:
U okviru Security Templates idite desni klik na folder u okviru koga zelite da kreirate novi timplejt i onda kliknite **New Template**. U **Template Name** polju unesite naziv novog timplejta, a u **Description** polju unesite korisne informacije za timplejt koji kreirate. U levom delu prozora dvoklik na novokreirani timplejt da bi ga otvorili. Selektujte sigurnosno polje kao sto je redzistri i onda ispodesavajte sigurnosna podesavanja u desnom delu prozora.
Drugi nacin i mnogo preporucljiviji je da uzmete neki predefinisani timplejt i sacuvate ga kao novi fajl i onda ga editujete po potrebi: Otici na **C:\WINDOWS\security\templates** i desni klik na zeljeni predefinisani timplejt i **save as** i samo unesite naziv novog fajla (tj sigurnosnog timplejta) i onda samo save. U levom delu prozora dvoklik na novokreirani timplejt da bi ga otvorili. Selektujte sigurnosno polje kao sto je redzistri i onda ispodesavajte sigurnosna podesavanja u desnom delu prozora.
Da vidimo sada kako se sve ovo ponasa na redzistri kljucevima. U levom delu prozora dvoklik na zeljeni timplejt i onda klik na **Registry** i pojavice vam se lista reg kljuceva u desnom delu prozora. Da bismo dodali kluc ovoj listi, idemo desni klik na registry i samo **Add Key**. Posto lista vec obuhvata sve kljuceve HKLM-a, napravicemo izuzetak ko dpodesavanja koja timplejt odredio za **HKLM\SOFTWARE i HKLM\SYSTEM**. Da bismo editovali kljuc idemo desni klik i selektujemo neku od sledecih opcija.

- **Configure This Key Then Propagate Inheritable Permissions To All Subkeys** - Kljucev podkljuc nasledjuje sigurnosna podesavanja kljuca predpostavljajuci da ta sigurnosna podesavanja podkljuca ne blokiraju nasledjivanje. U slucaju da dodje do konflikta, dozvole podkljuceve dozvole zamenjuju dozvole nasledjene od strane maticnog kljuca

- **Replace Existing Permissions On All Subkeys With Inheritable Permissions** - Dozvole kljuca u potpunosti zamenjuju sve dozvole njegovog podkljuca, sto znaci da ce svaka podkljuceva dozvola biti identicna dozvolama maticnog kljuca.

- **Do Not Allow Permissions On This key To Be Replaced** - Selektujte ovu opciju ako necete da podesavate dozvole kljuceva i podkljuceva.

5. Konfigurisanje računara i sigurnosne novotarije.

5.1 Analiziranje i sigurnosno konfiurisanje

Security Configuration and Analysis omogucava da uporedimo trenutno stanje sigurnosnih podesavanja sa podesavanjima zadatih preko sigurnosnih timplejtova.Ova analiza mogu biti odlican pokazatelj greski i inicijator resavanja istih. Na sledeci nacin se vrsi analiza sigurnosti upotrebom Security Configuration and Analysis alatke:
Idemo desni klik na **Security Configuration and Analysis** i klik na **Open Database**. Kada smo dospeli u Open Database prozoru, mozemo uraditi sledece dve stvari:

- **Da bismo kreirali novu Analysis bazu podataka**, u polje File Name upisemo naziv nove baze podataka i idemo na Open i onda Import Template prozoru selektujemo timplejt i kliknemo na Open.

- **Da bismo otvorili postojecu Analysis bazu podataka**, kliknucemo na Analyse Computer Now i prihvatiti defaultni log fajl ili odrediti novi.

Na taj nacin ce Security Configuration and Analysis uporediti trenutnu sigurnost racunara sa onom koja je dobijena kao rezultat analize baze podataka.Ukoliko ste imporotvali veci broj sigurnosnih timplejtova u bazu podataka,svi ce biti spojeni u jedan jedini timplejt. Ukoliko to izazove neki konflikt,poslednji ucitani timplejt ima prednost (znaci prvi timplejt leti napolje, poslednji ostaje). Nakon zavrsetka analize, izacice vam rezultati koji su isti kao i kod sigurnosnih timplejtova. Razlika je u tome sto Security Configuration and Analysis prikazuje sledece pokazatelje:

- **Crveni X** - Podesavanja su u bazi za analiziranje i kompu, ali te dve verzije ne ne odgovaraju jedna drugoj.

- **Zelena "kvachica"** - Podesavanja su u u bazi za analiziranje i kompui jedna drugoj drugima odgovaraju.

- **Znak pitanja** - Podesavanje nije u bazi za analiziranje i nije analizirano. To se desava verovatno zato sto korisnik nije imao dovoljni nivo dozvola da izvrsi pokretanje Security Configuration and Analysis.

- **Znak uzvika** - Podesavanja su u bazi za analiziranje i kompu, ali ne i u kompu. Redzistri kljuc se nalazi u bazi, ali ne i na kompu.

Bazu podataka mozemo apdejtovati klikom na dugme **Edit Security** i na taj nacin apdejtujemo bazu podataka a ne i sam timplejt..

5.2 Modifikovanje sigurnosne konfiguracije

Nakon sto smo napravili sigurnosni timplejt i analizirali ga, sada treba da ga prihvatimo tj ucitamo u komp, a to radimo na sledeci nacin:
Desni klik na **Security Configuration and Analysis** i idemo na **Open database**. U Open Database prozoru, mozemo uraditi sledece dve stvari:

- Da bismo kreirali novu bazu podataka, u polje File Name upisemo naziv nove baze podataka i idemo na Open i onda Import Template prozoru selektujemo timplejt i kliknemo na Open.
- Da bismo otvorili postojecu bazu podataka, uncemo naziv postojece baze podataka u File Name polje i onda Open.

Na kraju idemo desni klik na **Security Configuration and Analysis** i idemo na **Configure Computer Now** i onda prihvatimo defaultni log fajl ili odredimo novi.
Sve ovo je uglavnom primenljivo za **pojedinacne kompove**, ali ako zelimo da radimo sa sigurnosnim timplejtovima **na vecim mrezama**, treba da koristimo Group policy - kreiramo novi GPO i zatim ga editujemo. U GP editoru idemo desni klik -> Security Settings -> Import Policy -> oznacite zeljeni timplejt i Open.

5.3 Sigurnosne novotarije

Zajedno sa SP2 windoza je pored odredjenih sigurnosnih zakrpa i aplikacija dobila Security center i Firewall. A takodje je poprvalila i sledece bugove:
MS04-025 (867801) - Kumulativni Security Update za Internet Explorer •
MS04-024 (839645) - Ranjivost u Windows Shell Moze Izazvati Remote Code Izvrsenje •
MS04-023 (840315) - Ranjivost u HTML Help Moze Izazvati Code Izvrsenje •
MS04-022 (841873) - Ranjivost u Task Scheduler Moze Izazvati Code Izvrsenje •
MS04-018 (823353) - Kumulativni Security Update za Outlook Express •
MS04-016 (839643) - Ranjivost u DirectPlay Moze Izazvati Denial of Service •
MS04-015 (840374) - Ranjivost u Help u Support Center Moze Izazvati Remote Code Izvrsenje •
MS04-014 (837001) - Ranjivost u the Microsoft Jet Database Engue Moze Izazvati Code Izvrsenje •
MS04-013 (837009) - Kumulativni Security Update za Outlook Express •
MS04-012 (828741) - Kumulativni Update za Microsoft RPC/DCOM •
MS04-011 (835732) - Security Update za Microsoft Windows •
MS04-007 (828028) - ASN.1 Ranjivost Moze Izazvati Code Izvrsenje •
MS04-004 (832894) - Kumulativni Security Update za Internet Explorer •
MS04-003 (832483) - Buffer Overrun u MDAC Function Moze Izazvati Code Izvrsenje •
MS03-051 (813360) - Buffer Overrun u Microsoft FrontPage Server Extensions Moze Izazvati Code Izvrsenje •
MS03-049 (828749) - Buffer Overrun u the Workstation Service Moze Izazvati Code Izvrsenje •
MS03-048 (824145) - Kumulativni Security Update za Internet Explorer •
MS03-045 (824141) - Buffer Overrun u the ListBox u u the ComboBox Control Moze Izazvati Code Izvrsenje •
MS03-044 (825119) - Buffer Overrun u Windows Help u Support Center moze voditi do to Sistemskog greske •
MS03-043 (828035) - Buffer Overrun u Messenger Service Moze Izazvati Code Izvrsenje •
MS03-041 (823182) - Ranjivost u Authenticode Verification Moze Dozvoliti Remote Code Izvrsenje •
MS03-040 (828750) - Kumulativni Patch za Internet Explorer •

MS03-039 (824146) - Buffer Overrun u RPCSS Service Moze Izazvati Code Izvrsenje •
MS03-034 (824105) - Flaw u NetBIOS Voditi ka Razotkrivanju informacija •
MS03-032 (822925) - Kumulativni Patch za Internet Explorer •
MS03-030 (819696) - Neoznacen Buffer u DirectX Moze Omoguciti Sistemski Kompromis •
MS03-027 (821557) - Necekiran Buffer u Windows Shell Moze Omoguciti Sistemsku grsku •
MS03-026 (823980) - Buffer Overrun u RPC Uterface Moze Izazvati Code Izvrsenje •
MS03-024 (817606) - Buffer Overrun u Windows Voditi ka Propadanju Podataka •
MS03-023 (823559) - Buffer Overrun u HTML Converter-u Moze Izazvati Code Izvrsenje •
MS03-021 (819639) - Flaw u Windows Media Player Moze Dozvoliti Pristup Media Library •
MS03-020 (818529) - Kumulativni Patch za Internet Explorer •
MS03-018 (811114) - Kumulativni Patch za Internet Information Service •
MS03-015 (813489) - Kumulativni Patch za Internet Explorer •
MS03-014 (330994) - Kumulativni Patch za Outlook Express •
MS03-013 (811493) - Buffer Overrun u Windows Kernel Message Hulug Moze Dovesti do Podizanje Privilegija •
MS03-010 (331953) - Flaw u RPC Endpout Mapper Moze Izazvati Denial of Service Attacks •
MS03-008 (814078) - Flaw u Windows Script Engue Moze Izazvati Code Izvrsenje •
MS03-007 (815021) - Neoznacen Buffer u Windows Component Moze Izazvati Gresku u Serveru •
MS03-005 (810577) - Microsoft Security Bulletin MS03-005 •
MS03-004 (810847) - Kumulativni Patch za Internet Explorer •
MS03-001 (810833) - Neoznacen Buffer u Locator Service Voditi ka Code Izvrsenju •
MS02-072 (329390) - Neoznacen Buffer u Windows Shell Moze Omoguciti sistemsku gresku •
MS02-071 (328310) - Flaw u Windows WM_TIMER Message Hulug Moze Omoguciti Podizanje Privilegija •
MS02-070 (329170) - Flaw u SMB Signug Moze Omoguciti da Group Policy bude Modifikovan •
MS02-068 (324929) - Kumulativni Patch za Internet Explorer •
MS02-066 (328970) - Kumulativni Patch za Internet Explorer •
MS02-063 (329834) - Neoznacen Buffer u PPTP Implementation Moze Omoguciti Denial of Service Attacks •
MS02-062 (327696) - Kumulativni Patch za Internet Information Service •
MS02-055 (323255) - Neoznacen Buffer u Windows Help Facility Moze Omoguciti Code Izvrsenje •
MS02-050 (Q329115) - Certificate Validation Flaw Moze Omoguciti Prevaru Identiteta

5.4 Security Center

Security Centar je po meni zanimljivo zamisljen ali je jako lose odradjen. Na svakom kompu koji obradjujem, ja iskljucim odmah po instalu wina taj Security Centar. Al da pomenem sta sve u sebi ima, onima koji ga drze na svom kompu. On vrsi nadgledanje sledece tri win komponente: **Windows Firewall, Automatic Updates, Virus protection**. Upozorava vas da izvrsite apdejt ukoliko je update baza zastarela. Security centar mozete kontrolisati preko Active Directory Group policy opcija. U redzistriju pronadjite sledeci path:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center i tu mozete izvrsiti sledeca podesavanja

AV - Antivirus ; **FW** - firewall ; **WSC** - Windows Security Center ; **AU** - Automatic Update

Naziv kljuca	Vrsta	Vrednost
AntiVirusDisableNotify	REG_DWORD	0x00 - Disable AV alerts 0x01 - Prikazi AV alerts
AntiVirusOverride	REG_DWORD	0x00 - WSC nadgleda AV 0x01 - WSC ne nagleda AV
FirewallDisableNotify	REG_DWORD	0x00 - Disable FW alerts 0x01 - Prikazi FW alerts
FirewallOverride	REG_DWORD	0x00 - WSC nadgleda FW 0x01 - WSC ne nagleda FW
UpdatesDisableNotify	REG_DWORD	0x00 - Disable AU alerts 0x01 - Prikazi AU alerts

5.5 Windows Firewall

Windows Firewall je po meni pravi shit, i topla preporuka je da korisnite neki third party FW, a ne ovaj Windowsov, mada ja uopste ni ne koristim firewall :> Windozin fajer vol mozete konfigurisati preko Firewall Group policy podesavanja ili putem sledecih metoda:

- **Unattended - setup answer file** - Znaci preko unattend.txt fajla mozete iskonfigurisati fw i tek onda pristupiti instalaciji i uzivati skrstenih ruku.

- **Netfw.inf** - Podesavanje FW-a preko ovog inf fajla su ekvivalentna podesavanju koja vrsimo preko Windows Firewall Group Policy-a

- **Netsh Script** - Mozete napraviti batch skriptu koja ce sadrzati set netsh.exe komandi putem kojih mozemo podesiti Windows Firewall, dozvoljene portove itd.

- **Custom configuration programs** - Koristi API za konfiguraciju Firewalla.

Ako vas smori FW kao i mene mozete ga iskljuciti tako sto odete u servise (services.msc) i pronadjete Windows firewall - stopirate ga i diseblujete.