

# **Deo I**

## **Bezbednosna rešenja**

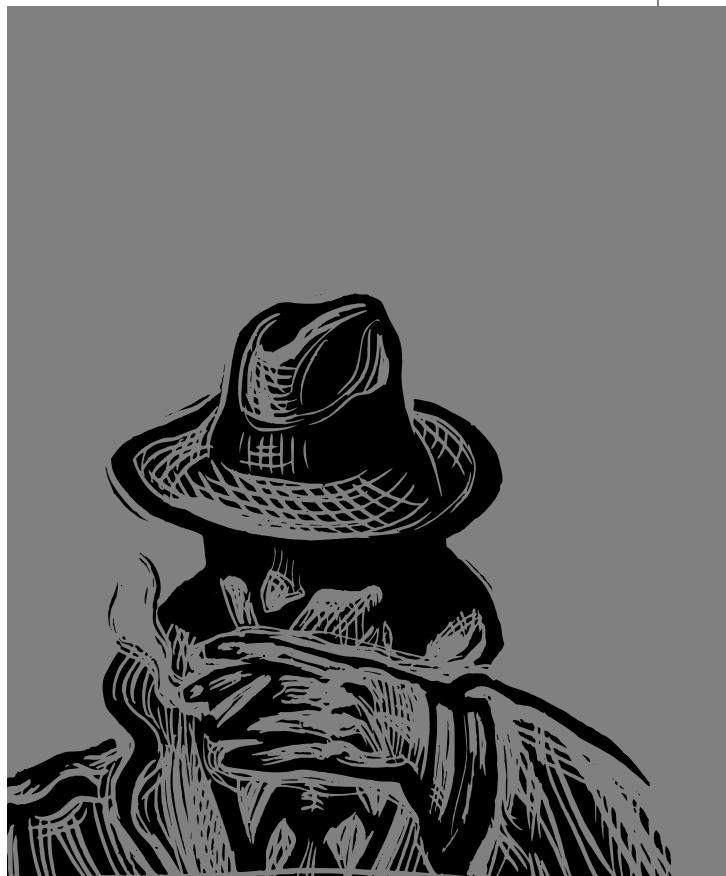
- 1** Bezbednost Windows Servera 2003
- 2** Implementacija bezbednih bežičnih tehnologija
- 3** Integracija inteligentnih kartica i bezbednih tehnologija pristupa

# 1

## Bezbednost Windows Servera 2003

IT administratori se suočavaju sa brojnim izazovima. Jedan od najvećih zadataka danas predstavlja bezbedno okruženje. Kompanije su mnogo popustljivije u dozvoljavanju partnerima da pristupe podacima na njihovim mrežama. Istovremeno, kompanije su mnogo strože kada se radi o bezbednosti tih podataka i komunikacija. Izazov za IT profesionalca je pronaći ravnotežu između upotrebljivosti i bezbednosti. Nekada, Microsoft nije bio od velike pomoći u ovoj "areni". Ranije verzije Windowsa su imale brojne "pukotine" u bezbednosti, što je računarska industrija sa zadovoljstvom reklamirala. S obzirom na to da se ogroman broj Windows računara koristi širom sveta, hakeri koji su znali kako ovi računari rade, zadavali su najjači udarac kada bi napali Windows.

Microsoft je napravio ogroman napredak u unapredavanju bezbednosti sopstvenih operativnih sistema i aplikacija. Svi softveri moraju da prođu rigorozne testove da bi se proverile sve poznate pukotine, osetljivost bafera i ostala potencijalna pitanja u vezi sa bezbednošću pre nego što se proizvod pojavi na tržištu. Windows 2003 je pravljen na samom početku ovog fokusiranja na bezbednost, tako da je pokupio sve prednosti izazvane povećanjem "svesti" Microsofta o potrebi proizvođenja bezbednih softvera.



### Ovo poglavlje sadrži

Poboljšavanje standardnog podešavanja bezbednosti u Windowsu 2003	6
Bezbednost svih ulaza	9
Identifikaciju konekcije pomoću dva faktora provere identiteta	14
Najbolji načini	
Integritet servera sertifikata	14
Korišćenje šablon za poboljšanje upotrebe i upravljanja	16
Revizija konfiguracije	17
Obezbeđivanje fajl sistema	20
Obezbeđivanje web servisa	22
Održavanje tajnosti fajlova pomoću EFS-a	24
Neprobojni scenario	26

## Poboljšavanje standardnog podešavanja bezbednosti u Windowsu 2003

Da bi se poboljšala bezbednost Windows Servera 2003, Microsoft je smanjio potencijalnu oblast napada u operativnom sistemu. To je urađeno

- Određivanjem strožih pravila standardnog podešavanja Access Control Lists (ACL) fajl sistema
- Redizajniranjem IIS-a
- Pružanjem sistematskih načina za konfigurisanje servera zasnovanih na prethodno određenim funkcijama
- Smanjivanjem ukupnog broja servisa
- Smanjivanjem broja servisa koji se pokreću po standardnom podešavanju
- Smanjivanjem broja servisa koji se pokreću kao sistem

U Windows Serveru 2003, Microsoft je isključio 19 servisa i modifikovao nekoliko servisa tako da se pokreću sa nižim privilegijama. Na primer, instaliranjem Windows Servera 2003 neće se automatski instalirati i IIS 6. Morate izričito da ga označite i instalirate ili da izaberete Web Server kao sistemsku funkciju preko Configure Your Server Wizard. Kada se server nadograditi Windows Serverom 2003, IIS 6 će, po standardnom podešavanju, biti isključen. Ako je IIS 6 instaliran, po standardnom podešavanju će biti blokiran. Nakon instaliranja, IIS 6 će prihvataći zahteve samo za statične fajlove. Ako želite da IIS 6 radi sa dinamičkim sadržajem, morate ga na taj način instalirati. Svi tajm-auti i parametri su podešeni na vrlo agresivni nivo zaštite. IIS 6 se, takođe, može isključiti korišćenjem grupnih pravila Windows Servera 2003, kako bi "nevaljali" administratori bili sprečeni da otvore neautorizovane web servere.

Windows 2003 ima "snažnije" standardno podešavanje ACL-a u fajl sistemu. To, sa druge strane, rezultira "snažnijim" standardnim podešavanjem ACL-a u deljenju fajlova. Na primer, grupa Everyone je ukljonjena iz standardnog podešavanja ACL-a. Napravljena su dva nova korisnička naloga za pokretanje servisa sa nižim nivoima privilegija. Na taj način se sprečava "ranjivost" servisa pri pokušaju da ga neko upotrebii za preuzimanje sistema. DNS Client i svi IIS Worker Processes se sada pokreću pomoću novog Network Service naloga. Telnet se pokreće pomoću novog Local Service naloga.

Windows 2003 je napravljen kao bezbedan sistem. Sistem instalira samo one komponente koje su neophodne za negov rad, bez instaliranja dodatnih servisa po standardnom podešavanju. Windows 2003 je podešen tako da eliminiše veliki broj potencijalnih rupa u bezbednosti, a to znači ne podržava "zaostavštinu" operativnih sistema koji su poznati po tome što im je bezbednost vrlo niska. Tokom instaliranja Windowsa 2003, sistem će Vas upozoriti da neće moći da identificuje klijente Windowsa 9x i Windowsa NT 4.0 ukoliko ne instaliraju Service Pack 3. To se dešava zbog toga što Windows 2003 postavlja dva specifična parametra u Domain Controller Security Policy:

- Microsoft mrežni server: digitalni znak komunikacije (uvek) - Enabled
- Bezbednost mreže: LAN Manager Authentication nivo - odgovara samo na Send HTML

Mada se ovi parametri mogu promeniti tako da omoguće ranijim operativnim sistemima da izvrše identifikaciju, ne preporučujemo Vam da to uradite. To bi ponovo otvorilo rupe u bezbednosti, a ovo pravilo je upravo dizajnirano da ih zatvori. Mnogi administratori će se sećati dana kada su web sajтовi mogli da objave LanMan (LM) zahteve hosta, a host bi ponudio korisničko ime i LM šifrovani (heš) lozinku. LM heš-funkcija je veoma slabo šifrovana da može biti slomljena brzo na silu (brute force attack). Mada je heš-funkcija smeštena u nereverzibilnom šifrovanju, algoritam šifrovanja je veoma poznat. Ako imate program za generisanje lozinke i primenite algoritam na njega, rezultat možete da uporedite sa ukradenom heš-funkcijom i vidite da li se poklapaju. Ako se poklapaju, saznaćete izvornu lozinku i sistem će biti ugроžen. To može biti izuzetno brzo ukoliko lozinka postoji u rečniku. Kada izlazite izvan područja Windowsa 2003, najbolje je da isključite lokalnu memoriju u kojoj su smeštene LM heš-funkcije na svim sistemima u mreži, preko Group Policy Objecta (GPO). Da biste odredili podešavanje grupnih pravila koji ograničavaju memoriju LM Hash Value, uradite sledeće;

1. Za Group Policy objekat izaberite Computer Configuration, Windows Settings, Security Settings, Local Policies, a zatim kliknite na Security Options.
2. U listi raspoloživih pravila kliknite dva puta Network Security: Do Not Store LAN Manager Hash Value on Next Password Change.
3. Kliknite Define This Policy Setting, izaberite Enabled, a zatim kliknite OK.

## Poboljšanja u odnosu na Windows 2000

Najbolje poboljšanje bezbednosti u odnosu na Windows 2000 se ne tiče tehnologije, već procedure. Windows 2000 instalira, po standardnom podešavanju, Internet Information Server, a IIS instalira podsisteme OS2 i Posix i nudi veoma ograničen uvid u implikacije koje proizilaze iz instaliranja različitih servisa i aplikacija. Sa druge strane, Windows 2003 uvodi Configure Your Server Wizard. Ovaj Wizard se pokreće po standardnom podešavanju kada se Windows 2003 prvi put instalira. Windows 2003 će Vas "pitati" kakva će biti funkcija servera i u skladu sa tim će izvršiti odgovarajuće izmene u sistemu. Fajlovi će biti instalirani, bezbednost servisa podešena, a administrator će biti zadovoljan zato što zna da sistem nije instalirao nijedan nepotreban servis. Na taj način se eliminiše glavni uzrok nebezbednosti sistema - pogrešno konfigurisanje.

## Nove bezbednosne tehnologije uvedene u Windows 2003

Jedna od novih tehnologija uvedena u Windows 2003 je Internet Information Services 6. IIS je redizajniran u Windows Serveru 2003 radi unapređivanja bezbednosti web orijentisanih transakcija. IIS 6 omogućava izdvajanje pojedinačne web aplikacije u poseban web servis. Tako se sprečava da jedna aplikacija ometa druge aplikacije koje se izvršavaju na istom web serveru. Isto tako, IIS omogućava ugrađenoj sposobnosti monitoringa da pronađe, popravi ili izbegne greške u web aplikaciji. U IIS-u 6, kodovi dodatne aplikacije se izvršavaju u izdvojenom postupku obrade, za koji se sada koristi prijavni nalog sa manjim privilegijama, Network Service. Izdvajanje postupka obrade omogućava ograničavanje web sajta ili aplikacije na njihov osnovni direktorijum, kroz Access Control Lists (ACL). Tako se sistem štiti od pokušaja da neko "uđe" u fajl sistem i pokrene izvršavanje skripta ili drugih ugrađenih kodova.

Windows 2003, takođe, ima poboljšanu bezbednost mrežne komunikacije, a ostvaruje se kroz podršku strožeg protokola provere identiteta kao što su 802.1 (WiFi) i Protected Extensible Authentication Protocol (PEAP). Internet Protocol Security (IPSec) je unapređen i dalje integriran u operativni sistem da bi se poboljšalo LAN i WAN šifrovanje podataka.

Microsoft je uveo Common Language Runtime (CLR) softverski mehanizam u Windows Server 2003 da bi unapredio pouzdanost i stvorio sigurnije okruženje za programiranje i upotrebu računara. CLR utvrđuje da li aplikacije mogu da se izvršavaju bez grešaka i proverava njihovu bezbednost kako bi bilo sigurno da kodovi neće izvršavati nedozvoljene operacije. CLR smanjuje broj bagova i rupa u bezbednosti prouzrokovanih uobičajenim greškama u programiranju. To rezultira manjim mogućnostima da hakeri ugroze sistem.

Još jedna tehnologija uvedena u Windows 2003 je koncept Forest Trusts. Windows Server 2003 podržava među-forest trusts, omogućavajući kompanijama da se bolje integrišu sa ostalim kompanijama koje koriste aktivni direktorijum. Podešavanje među-forest trustsa sa partnerskim aktivnim direktorijumom omogućava korisnicima bezbedan pristup izvorima informacija bez gubljenja pogodnosti jednog prijavljivanja. Ova osobina Vam omogućava upotrebu ACL-a zajedno za korisnicima ili grupama iz partnerskog aktivnog direktorijuma. Ova tehnologija predstavlja veliku prednost u situacijama kada jedna kompanija preuzima drugu. Postavljanje među-forest trustsa omogućava da obe kompanije počnu odmah da dele izvore informacija na potpuno bezbedan način.

Ideja jednog prijavljivanja je unapređena uvođenjem Credential Managera. Ova tehnologija obezbeđuje bezbedno smeštanje korisničkih imena i lozinki, kao i linkova do sertifikata i ključeva. Tako je korisnicima omogućena doslednost jednog prijavljivanja. Jedno prijavljivanje omogućava korisnicima da pristupaju izvorima informacija preko mreže, a da pri tom ne moraju stalno da dokazuju svoj identitet.

Windows Server 2003 podržava Constrained Delegation. Delegacija (Delegation) u ovom kontekstu podrazumeva dozvoljavanje servisu da predstavlja korisnički ili računarski nalog da bi pristupio izvorima informacija na mreži. Ova nova osobina Windows Servera 2003 Vam omogućava da ovoj vrsti delegacije ograničite pristup samo na određene servise ili izvore informacija. Na primer, servis koji koristi delegaciju da bi pristupio sistemu u ime korisnika, sada može biti ograničen tako da predstavlja korisnika samo pri povezivanju sa jednim određenim sistemom, a ne i sa ostalim računarima ili servisima u mreži. Ovo je slično konceptu ograničavanja korisnika da se "zakači" na neku od zabranjenih listi u sistemu.

Protocol Transition je tehnologija koja dozvoljava servisu da identitet korisnika konvertuje tako da bude zasnovan na Kerberosu, a da pri tom ne mora da zna lozinku korisnika ili da zahteva od korisnika proveru identiteta preko Kerberosa. Tako se korisniku Interneta omogućava provjeru identiteta pomoću uobičajenih metoda i dobijanje Windows identiteta. Ova tehnologija je sada dostupna u Windowsu 2003. To može biti veoma korisno za kompanije koje planiraju da koriste Kerberos kao centralnu tačku provere identiteta za oba operativna sistema, Windows i Linux.

Windows Server 2003 sada nudi .NET Passport Integration sa aktivnim direktorijumom. Tako se omogućava Passport orijentisana provjeru identiteta koja će obezbediti partnerima i klijentima jedno prijavljivanje za izvore informacija i aplikacije zasnovane na Windowsu. Upotrebom .NET Passport servisa kompanije će smanjiti troškove upravljanja korisničkim imenima i lozinkama za aplikacije koje imaju veliki broj spoljašnjih korisnika. Microsoft

je uložio puno napora da bi osigurao da .NET Passport informaciju budu bezbedno smeštene, da bi unapredio pouzdanost u industriji i pomogao u razvijanju tehnologije.

Mada Windows 2000 podržava šifrovanje direktorijuma, Windows Server 2003 sada dozvoljava šifrovanje offline fajlova i direktorijuma upotrebom EFS-a. Offline Files, ili keširanje na strani klijenta, postoji u Windowsu 2000 i omogućava mobilnim korisnicima da rade na lokalnim kopijama fajlova kada nisu povezani sa mrežom. Kada se korisnik ponovo poveže sa serverom, sistem usklađuje izvršene izmene sa starom verzijom dokumenta na serveru. Tako se obezbeđuje konstantna zaštita fajlova dok su oni keširani lokalno, na mobilnom računaru.

U Windowsu 2003 je obezbeđena bolja tehnologija šifrovanja za EFS. Windows Server 2003 sada podržava šifrovanje za EFS koje je "jače" od standardno podešenog Data Encryption Standard (DESX) algoritma. Po standardnom podešavanju, EFS će koristiti Advanced Encryption Standard (AES-256) za sve šifrovane fajlove. Klijenti, takođe, mogu da koriste Federal Information Processing Standards (FIPS) 140-1 algoritme, kao što je 3DES algoritam, koji se takođe nalazi u Windowsu XP Professional.

## Bezbednost svih ulaza

Danas je ceo svet u potrazi za bezbednošću. Kako u svetu sve više dolazi do povezivanja informacija, tako se sve više pojavljuje pitanje privatnosti tih informacija. Vlada se u više mandata bavila pitanjima bezbednosti informacija identiteta u oblasti medicine, odnosno istorija bolesti i informacija koje se odnose na decu.

Trgovina na Webu je u prvi plan izbacila pitanja da li su informacije o kreditnim karticama bezbedno smeštene i da li su online transakcije sigurne. Ova pitanja su "izrodila" mnoštvo tehnologija, a svetske korporacije su ih prihvatile zbog sopstvene unutrašnje bezbednosti. Kako pristup informacijama postaje sve lakši i lakši, tako postaje sve teže i teže zaštiti podatke i njihovo prenošenje.

### Bezbednost i reputacija kompanije

Ako kompanija želi da zadrži klijente na današnjem tržištu, onda klijenti moraju da veruju toj kompaniji. Velike online trgovine zavise od toga da li klijenati imaju poverenja u njihovu bezbednost, kako bi nastavili da posluju sa njima. Sve dok klijenti veruju da se informacije o njihovim finansijama bezbedno prenose i smeštaju, oni će nastaviti da posluju sa online kompanijom.

Ukoliko neka od online trgovina bude ugrožena, na primer krađom brojeva kreditnih kartica, to može da uništi tu kompaniju. Reputacija kompanije je direktno povezana sa njenom bezbednošću. Greške u bezbednosti najčešće vode do sloma kompanije.

## Implementacija Transport Layer Security

Koncept Transport Layer Security (TLS) podrazumeva da komunikacija između mrežnih uređaja treba da se obavlja na takav način koji će spričiti svaki drugi uređaj, koji može da prekine tu komunikaciju, da upotrebi informacije. TLS, koji je sličan SSL-u, se zasniva na x.509 sertifikatu koji mora biti objavljen od strane priznatog Certificate Authority (CA) - autoriteta za sertifikate. TLS može da uradi sledeće:

- Da otkrije neispravnu poruku
- Da otkrije presretnutu poruku
- Da otkrije falsifikovanu poruku

Da biste upotrebili TLS za klijent/server komunikaciju, prođite kroz sledeće korake:

1. Potvrdite spremnost za prenos i stvaranje šifrovanog kanala.
2. Proverite identitet strana.
3. Razmenite informacije o ključu.
4. Razmenite podatke aplikacije.

Po standardnom podešavanju, TLS će prihvati bilo koju šifru; zato ga možete zaključati pomoću GPO-a, da bi se ograničio mogući izbor šifara, kroz modifikaciju sledećeg Registry ključa:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Security Providers\SCHANNEL\Ciphers

Pronaći ćete listu sa više mogućih šifara koje možete uključiti ili isključiti, u zavisnosti od toga šta Vam odgovara.

TLS Handshake Protocol podrazumeva sledeće korake:

1. "Klijentov pozdrav" se šalje iz računara klijenta do servera, zajedno sa slučajnom vrednošću i listom podržanih šifara.
2. "Serverov pozdrav" se šalje kao odgovor klijentu, zajedno sa slučajnom vrednošću servera.
3. Server šalje svoj sertifikat klijentu da bi potvrdio autentičnost, a isto tako može da zahteva sertifikat od klijenta. To rezultira porukom o "završenom pozdravu servera". Klijent šalje sertifikat ukoliko je server to zahtevao.
4. Klijent zatim stvara slučajni Pre-Master Secret i šifruje ga preko javnog ključa iz sertifikata servera. Ovaj šifrovani Pre-Master Secret se šalje serveru.
5. Nakon prijema Pre-Master Secreta i server i klijent generišu ključeve sesije i Master Secret na osnovu Pre-Master Secreta.
6. Klijent šalje serveru poruku o "promeni specifikacije šifre" da bi ukazao da klijent počinje da koristi nove ključeve sesije za šifrovanje poruka. Klijent, takođe, šalje poruku da je "klijent završio".
7. Server dobija poruku o "promeni specifikacije šifre" i menja stanje svog sloja zaštite tako da koristi simetrično šifrovanje na osnovu ključeva sesije. Server šalje klijentu poruku da je "server završio".
8. Klijent i server sada mogu da razmenjuju podatke preko sigurnog kanala koji su uspostavili. Svi podaci i komunikacije koji se šalju od klijenta do servera i od servera do klijenta su šifrovani pomoću ključa sesije.

## Zahtevanje digitalnog potpisa

Starija implementacija Small Message Block (SMB) komunikacija je bila osetljiva na nešto što se naziva *posrednički napad* (man-in-the-middle attack). Posrednički napadi se pojavljuju kada napadač, maskiran kao jedna od legitimnih strana, ubacuje poruke u komunikacioni kanal. To napadaču omogućava da šalje sopstvene akreditive, tako da ostali hostovi prihvataju njegovu konekciju. Postavljanjem digitalnog potpisa u svaki SMB, koji verifikuju i server i klijent, stvara se uzajamna identifikacija koja proverava validnost i servera i klijenta. Ako ovakvo obezbeđenje postoji na serveru, klijenti moraju da podrže digitalno potpisivanje komunikacija, jer u suprotnom neće moći da komuniciraju sa serverom.

Ovakvo podešavanje bezbednosti se može konfigurisati u Default Domain Controller Security Settingsu odabiranjem Security Settings/Local Policies/Security Options/Microsoft Network Server: Digitally Sign Communications - Enabled (uvek).

## Upotreba PKI-a

Naravno da nije iznenađujuće što tehnologije zasnovane na sertifikatima zahtevaju pristup sertifikatima. Još određenije, sertifikatima koje je objavio autoritet za sertifikate kojem se veruje. Kompanije mogu da izaberu neki od spoljašnjih autoriteta za sertifikate kao što su Verisign, SecureNet ili Globalsign. Jedna od prednosti korišćenja spoljašnjih autoriteta za sertifikate je što sa njima, kao glavnim autoritetima kojima verujete, dobijate već učitan Internet Explorer. To znači da klijenti ne moraju da kontaktiraju ove glavne (Root) CA-e i nude korisnicima da prihvate sertifikat. Kompanija ima i drugu opciju, a to je da ustanovi sopstveni autoritet za sertifikate. To može biti Root CA (osnovni) ili Enterprise CA (CA preduzeća), koji su napravljeni na osnovu sertifikata dobijenog od drugog Root CA-a.

Ako kompanija želi da objavi sopstvene sertifikate, u računar klijenta se prethodno može učitati sertifikat preko parametra GPO. Na primer, ako kompanija želi da koristi digitalne sertifikate u svom intranetu, ona može da pošalje sertifikat servera do klijenta i odredi server kao Intermediate Certification Authority. Da biste poslali sertifikat klijentima, uradite sledeće:

1. Pokrenite editor GPO.
2. Izaberite User Configuration, Windows Settings, Internet Explorer Maintenance, Security, Authenticode Settings.
3. Izaberite Import Existing Authenticode Settings.
4. Kliknite Modify Settings.
5. Kliknite Import. Pokrenućete Import Certificates Wizard.
6. Kliknite Next.
7. Kliknite Browse, a zatim potražite fajl sertifikata. Izaberite Open, a onda kliknite Next.
8. Izaberite Browse i označite odgovarajuće mesto gde ćete smestiti sertifikat.
9. Izaberite Next, a zatim kliknite Finish.

Čarobnjak će Vas obavestiti da ćete upravo instalirati sertifikat, navodeći određeni izvor. Ako je ta informacija tačna, označite "yes". Čarobnjak će Vas obavestiti da je sertifikat uspešno instaliran.

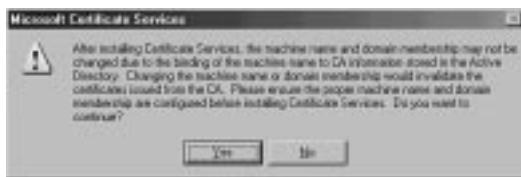
## Instaliranje servisa sertifikata

Instaliranje servisa sertifikata u Windows Server 2003 zahteva server Windows 2003 i dodavanje komponente Certificate Services na server. Proces dodavanja Certificate Servicesa Windowsu 2003 podrazumeva sledeće:

1. Izaberite Start, Control Panel, Add or Remove Programs.
2. Kliknite Add/Remove Windows Components.
3. Potvrdite polje Certificate Services.
4. Pojaviće se okvir za dijalog, kao što je prikazano na slici 1.1, sa upozorenjem da nećete moći da promenite ime računara ili naziv domena nakon instaliranja Certificate Servicesa. Kliknite Yes da bi se proces instaliranja nastavio.

**Slika 1.1**

Upozorenje  
Certificate Services.



5. Kliknite Next.

6. Sledеći ekran, prikazan na slici 1.2, omogućava Vam da napravite vrstu CA-a, koja se zahteva. U ovom primeru izaberite Enterprise Root CA i kliknite Next.

**Slika 1.2**

Izaberite vrstu  
CA servera koja će  
biti instalirana.



7. Unesite neko uobičajeno ime za CA - na primer, CompanyABC Enterprise Root CA.
8. Unesite rok važnosti za Certificate Authority i kliknite Next. Nakon toga će biti napravljen kriptografski ključ.

**Ako je na serveru instaliran IIS, pojaviće se okvir za dijalog**

Ako je na serveru instaliran IIS, pojaviće se okvir za dijalog sa obaveštenjem da će IIS biti privremeno zaustavljen. Kada se pojavi pitanje da li se slažete da se IIS servis zaustavi i ponovo pokrene, izaberite Yes, osim ako je servis aktivan u trenutku instaliranja servisa sertifikata.

9. Unesite lokaciju za bazu podataka sertifikata, a zatim dnevnik rada baze podataka. Lokacija koju izaberete mora da bude bezbedna, da bi se sprečilo neovlašćeno pristupanje CA-u. Kliknite Next. CA komponente će biti instalirane.
10. Ako IIS nije instaliran, pojaviće se poruka, prikazana na slici 1.3, obaveštavajući Vas da će Web Enrollment biti isključen dok ne instalirate IIS. Ako se ova poruka pojavi, kliknite OK.

**Slika 1.3**

IIS upozorenje  
u proceduri  
instaliranja CA-a.



11. Kliknite Finish da biste završili postupak instaliranja.

## Važnost fizičke bezbednosti

Bezbednost mreže je potpuno beskorisna ako serveri nisu fizički bezbedni. Računari ne prepoznaju razliku između lokalne "provale" i legitimne upotrebe lozinke. Mada su poverljive informacije smeštene u aktivni direktorijum, ipak se aktivni direktorijum sastoji od baza podataka smeštenih na serverima. Ove informacije su postavljene u specifičnoj strukturi i osoba koja ima fizički pristup hard disku gde je smešten NTDS.DIT fajl i editor sektora može da ugrozi bezbednost baza podataka.

Serveri moraju uvek da budu smešteni u zaključanim centrima za bezbedne podatke. Pristup tim centrima mora da bude ograničen i nadgledan. Bezbednosni protokol [%systemroot%\System32\config\SecEvent.Evt] mora biti kopiran na dve odvojene lokacije da bi se sprečilo "provaljivanje". Aplikacije kao što je Microsoft Operations Manager, koja centralizuje upravljanje evidencijom događaja, su pogodne za ovakave zadatke. Implementacija servera za sistemsko evidentiranje, takođe, može biti od pomoći.

Pristup centrima sa bezbednim podacima mora da zahteva više oblika provere identiteta. Na primer, umesto da se oslonite samo na čitanje propusnice, brava bi mogla da se sastoji od kombinacije čitanja propusnice i unošenja PIN koda. Na taj način, krađa propusnice ne bi bila dovoljna za ugrožavanje centra sa bezbednim podacima.

## Najbolji načini

### **Integritet servera sertifikata**

Stvaranje internog servera sertifikata nije beznačajan događaj i mada se može uraditi kroz 11 relativno jednostavnih koraka zabeleženih u ovom poglavlju, organizacije moraju shvatiti veoma ozbiljno bezbednost servera sertifikata. Autoritet za sertifikate pruža bezbednost samo kada je integritet procesa stvaranja sertifikata osiguran. Ako svako može da dode do servera sertifikata organizacije i napravi sertifikat, onda niko ne može znati da li je sertifikat koji poseduje izdao pravi administrator ili neki neovlašćen pojedinac. Ako niko nije siguran u valjanost sertifikata, onda su bezbednost prenošenja podataka, provera identiteta prijave ili šifrovanje podataka veoma ugroženi.

Pošto je server glavnog sertifikata nadležan za ime domena organizacije (kao što je companyabc.com), ta organizacija nikako ne želi da njen server glavnog sertifikata bude ugrožen. Ako niko nije siguran da li je valjana provera identiteta zasnovana na sertifikatu za tu organizaciju, onda organizacija nema kredibilitet za bezbednost zasnovanu na sertifikatu zato što neko ko nema ovlašćen pristup serveru sertifikata može da objavi sertifikate izvan organizacije. Kada stvaraju servere glavnog sertifikata, mnoge velike organizacije dele taj zadatak na kreiranje sertifikata, upravljanje hardverom i sistemske operacije. Hardver je bezbedan na mestu gde je pristup strogo ograničen. Kreiranje sertifikata se mora obavljati na konzoli servera, bez podešavanja za udaljeno pristupanje. Pristup serveru zahteva prijavljivanje dva ili tri pojedincu koji će pristupiti odgovarajućim pomoćnim programima za kreiranje sertifikata. Svi koraci se snimaju kamerom i smeštaju na bezbedno mesto. Iako ceo ovaj postupak izgleda veoma složeno, uobičajen je za svaku organizaciju zato što štiti integritet sertifikata organizacije.

Velika pažnja se mora posvetiti osiguravanju da je proizvod Root CA-a urađen na bezbedan i proveren način. Ugrožavanje Root CA-a suštinski ugrožava svaku kompaniju i podređeni CA, koji su izgrađeni pomoću sertifikata objavljenih od strane Root CA-a. To, sa druge strane, ugrožava svaki sertifikat koji je objavljen u CA hijerarhiji.

### **Identifikujte konekciju pomoću dva faktora provere identiteta**

Korisničko ime i lozinka već dugo predstavljaju standarde za proveru identiteta korisnika. U Windowsu NT je ovaj proces unapređen dodavanjem naloga maštine koji je potrebno prijaviti domenu. Mada je to bilo dobro za prijavljivanje na domen, ipak se moglo zaobići spajanjem na mrežne resurse i izbegavanjem provere identiteta. Većini kompanija su potrebne strože metode provere identiteta. Posebno je kritično kada su u pitanju udaljeni korisnici. Skupove modema i VPN uređaje je relativno jednostavno pronaći. Zlonamerni hakeri mogu relativno nekažnjeno proći kroz ove uređaje. To nas dovodi do koncepta provere identiteta pomoću dva faktora kao što su inteligentne kartice i biometrička provera identiteta.

### **Upotreba intelligentnih kartica**

*Intelligentna kartica* je lako prenosiv programabilan uređaj koji se sastoji od integrisanog kola gde se informacije smeštaju i obrađuju. Intelligentne kartice su obično u formi

uređaja veličine kreditne kartice, koje se smeštaju u čitač, ali isto tako mogu biti uređaji zasnovani na USB-u ili integrisane u propusnice zaposlenih. Windows 2003 i Windows XP podržavaju inteligentne kartice kao metodu provere identiteta. Inteligentne kartice se kombinuju sa PIN-om, koji se može smatrati lozinkom, pa se tako dobija provera identiteta na osnovu dva faktora. Fizičko posedovanje inteligentne kartice i znanje PIN-a se moraju iskobinovati u uspešnu proveru identiteta.

Da bi koristio intelligentnu karticu, korisnik domena mora da ima sertifikat intelligentne kartice. Administrator mora da pripremi autoritet za sertifikate (CA) za izdavanje sertifikata pre nego što CA počne sa njihovim izdavanjem. Za CA je neophodno instalirati oba šablon sertifikata, Smart Card Logon i Enrollment Agent. Ako će se sertifikati intelligentne kartice koristiti za bezbedne e-mail poruke, onda administrator mora da instalira i šablon sertifikata Smart Card User.

Da biste konfigurisali Enterprise CA zasnovan na Windowsu za izdavanje sertifikata intelligentne kartice, uradite sledeće:

1. Prijavite se u Enterprise CA. Potrebno je da koristite nalog administratora domena.
2. U meniju Start izaberite Programs, Administrative Tools, Certification Authority.
3. U konzoli Certification Authority proširite Vaš domen, kliknite desnim tasterom miša kontejner Certificate Templates i izaberite New, Certificate Template to Issue.
4. U okviru za dijalog Enable Certificate Template označite Smartcard User i kliknite OK.
5. Kliknite desnim tasterom miša kontejner Certificate Template, a zatim kliknite Manage. Otvoriće se Certificate Templates MMC.
6. U Select Certificate Template MMC-u kliknite desnim tasterom miša Smartcard User i označite Properties.
7. Kliknite karticu Security. Kliknite dugme Add i izaberite grupu kojoj želite da omogućite pristup pomoću intelligentne kartice (u ovom primeru, grupa Smartcard Users, čiji su članovi zaposleni koji poseduju intelligentne kartice, biće dodata aktivnom direktorijumu).
8. Označite Read i Enroll iz Permissionsa, kao što je prikazano na slici 1.4, a zatim kliknite OK.

## Upotreba biometrike za poboljšanje bezbednosti

Biometrika se odnosi na jedinstvene biološke informacije koje se koriste za određivanje identiteta korisnika. Biometrika, kombinovana sa proverom identiteta pomoću korisničkog imena/lozinke, predstavlja autentifikaciju sa dva faktora, koja se ne može kopirati. Obrisak prsta, gustina kostiju i izgled mrežnjače oka se najčešće koriste kao biometričke metode provere identiteta.

Dodata biometrička rešenja predstavljaju dozvoljene mehanizme autentifikacije, koji funkcionišu zajedno sa postojećim protokolima provere identiteta u mrežnim operativnim sistemima. Tehnologije, kao što je skeniranje mrežnjače, su obično samostalni uređaji, dok čitači otiska prstiju mogu biti ugrađeni u tastasturu korisnika.

**Slika 1.4**

Dodavanje grupe čiji će se identitet proveravati pomoći inteligentne kartice.



## Korišćenje šablon za poboljšanje upotrebe i upravljanja

Jedan od glavnih ključeva uspešne bezbednosti je standardizacija aplikacije u pogledu pravila bezbednosti u okruženju. Windows 2003 nastavlja da podržava ovaj koncept koristeći Security Configuration i plug-in Analysis MMC. Ovaj plug-in Vam omogućava da konvertujete sopstvena pravila bezbednosti u fajl šablonu koji se može primeniti na ostale servere. Tako ćete biti sigurni da su serveri identično konfigurisani. To je posebno korisno za sisteme koji su konfigurisani tako da se nalaze izvan zaštitnog zida i nisu članovi domena aktivnog direktorijuma, pa se zbog toga njima ne može upravljati pomoću Group Policy Objectsa.

### Upotreba alata Security Configuration and Analysis

Alat Security Configuration and Analysis, kojem u Windowsu 2003 pristupate iz MMC Snap-in-a, je dizajniran tako da čita specifične bezbednosne informacije sa servera i upoređuje ih sa fajлом šablonu. To Vam omogućava da stvarate standardne šablone i posmatrate da li serverima u njihovom okruženju odgovaraju takva podešavanja.

Da biste izvršili analizu sistema, uradite sledeće:

1. Izaberite Start, Run, mmc.exe, a zatim kliknite OK da biste pokrenuli MMC Snap-in.
2. Dodajte alat Security Configuration and Analysis.
3. Kliknite desnim tasterom miša stavku Security Configuration and Analysis i izaberite Open Database.
4. Izaberite naziv baze podataka i kliknite Open.
5. Izaberite bezbednosni šablon, a zatim ga otvorite.

6. Kliknite desnim tasterom miša stavku Security Configuration and Analysis i izaberite Analyze Computer Now, a zatim kliknite OK.

Sistem će prikazati lokalno podešavanje bezbednosti, kao i preporuku šablonu iz baze podataka. Upoređivanjem lokalnog podešavanja sa standardnim šablonom koji je napravio administrator, podešavanje može biti doslednije, bez poništavanja bilo kojeg od zahtevanih lokalnih podešavanja bezbednosti.

## Upotreba bezbednosnih šablona

Grupe kao što su National Security Agency (NSA) ili National Institute of Standards and Technology (NIST) su napravile ono što su, po njihovom mišljenu, bezbednosni šabloni za funkcije kakve su Domain Controller, Web Server, Application Server i druge. Koristeći ove šablone kao početnu tačku, možete da napravite prilagođene šablone uzimajući u obzir savete NIST-a ili NSA-a. To će Vam puno olakšati pravljenje bezbednosnog šablonu, jer su ove grupe specijalizovane u poznavanju i razumevanju bezbednosti računara.

## Revizija konfiguracije

Kada "prodlete" kroz server i ustanovite da je stanje zadovoljavajuće, važno je da proverite sva podešavanja prema dodatnim alatima, kako biste bili sigurni da niste ništa propustili. Takođe, veoma je važno znati da Vaša mreža odgovara standardima priznatih bezbednosnih entiteta kao što su NSA ili NIST. Prema zahtevima postavljenim u Health Insurance Portability and Accountability Actu (HIPAA) ili Graham Leach Bliley Actu (GLBA), od mnogih kompanija se sada zahteva da pokažu dokumentaciju koja dokazuje da su preduzele sve neophodne korake u obezbeđivanju osetljivih informacija u njihovim mrežama. Dodatni alati za analizu omogućavaju objektivnu i nepristrasnu procenu bezbednosti mreže. Mada su neke od tehnologija procenjivanja vrlo potpune, one ne mogu da zamene proveru koje vrše respektibilne kompanije specijalizovane u reviziji bezbednosti mreže.

## Proveravanje bezbednosti sistema

Dnevnik zapisa dogadaja je odličan način praćenja aktivnosti na serveru. Pravila lokalne bezbednosti omogućavaju uključivanje ili isključivanje različitih kontrola događaja, a to će biti objašnjeno u sledećoj listi:

- **Audit account logon events (kontrolno praćenje događaja prijavnog naloga).** Ovaj parametar kontroliše svaku instancu prijavljivanja ili odjavljivanja korisnika na ili sa drugog računara, gde se taj računar koristi za proveravanje naloga. Događaji prijavnog naloga se generišu kada kontroler domena proverava identitet korisnika domena. Događaji se zapisuju u bezbednosni protokol kontrolera domena. Slično tome, prijavni događaji se generišu kada lokalni računar proverava identitet lokalnog korisnika. U ovom slučaju, događaji se zapisuju u lokalni bezbednosni protokol.
- **Audit account management (kontrolno praćenje upravljanja naloga).** Ovaj parametar kontroliše svaku instancu na kojoj je korisnički ili grupni nalog kreiran, promenjen ili izbrisana. Takođe, generiše događaje kada se korisničkom nalogu promeni ime i kada se nalog deaktivira ili aktivira. Podešavanje ili menjanje lozinke se, takođe, kontroliše.

- **Audit directory service access (kontrolno praćenje pristupanja servisu direktorijuma).** Ovaj parametar kontroliše svaki događaj pristupanja korisnika aktivnom direktorijumu koji ima sopstvenu kontrolnu listu pristupanja sistemu (System Acces Control List - SACL).
- **Audit object access (kontrolno praćenje objekta).** Ovaj parametar kontroliše događaj pristupanja korisnika objektu, kao što su fajl, folder, Registry key ili štampač, koji ima sopstvenu kontrolnu listu pristupanja sistemu (SACL).
- **Audit policy change (kontrolno praćenje promene pravila).** Ovaj parametar kontroliše slučajeve promene pravila u pravima koja su dodeljena korisniku, pravilima kontrole i pravilima poverenja.
- **Audit privilege use (kontrolno praćenje korišćenja privilegija).** Ovaj parametar kontroliše svaku instancu primene korisničkih prava.
- **Audit process tracking (kontrolisanje postupka praćenja).** Ovaj parametar kontroliše detaljno praćenje informacija o događajima kao što su aktiviranje programa, napuštanje postupka, rukovanje kopijama i indirektno pristupanje objektima.
- **Audit system events (kontrolno praćenje sistemskih događaja).** Ovaj parametar kontroliše događaj kada korisnik ponovo pokrene ili isključi računar ili kada se pojavi neki događaj koji utiče na bezbednosni sistem ili bezbednosni dnevnik zapisa.

## Korišćenje Microsoft Baseline Security Analyzera

Microsoft Baseline Security Analyzer je alat dizajniran tako da određuje koja su najnovija ažuriranja trenutno primenjena na sistem. MBSA izvršava ovaj zadatak pozivajući se na XML (Extensible Markup Language) fajl, pod nazivom mssecure.xml.

### MBSA i najnovija kopija mssecure.xml fajla

MBSA se spaja sa Microsoftovim web sajtom da bi "izvukao" najnoviju kopiju mssecure.xml fajla. Ako računar na kojem je MBSA pokrenut nema pristup Internetu, možete da preuzmete XML fajl i smestite ga na računar gde je MBSA pokrenut. Setite se da redovno ažurirate ovaj fajl, kako biste stalno bili u toku sa najnovijim ažuriranjima sistema.

Ovaj fajl se redovno ažurira od strane Microsofta, kako bi važio kao izveštaj za sve izvršene ispravke. Korišćenjem tehnologije HFNetChk, MBSA može da kontroliše odredišni sistem prema listi trenutnih ispravki. Ovaj XML fajl sadrži informacije o tome koja su bezbednosna ažuriranja na raspolaganju za određene Microsoftove prizvode, izvan operativnog sistema koji se u tom trenutku koristi. Fajl sadrži nazive i naslove biltena o bezbednosti, kao i detaljne informacije o specifičnim bezbednosnim ažuriranjima proizvoda, uključujući sledeće:

- Fajlove u svakom paketu ažuriranja
- Verzije i kontrolne sume
- Ključeve Registrya koje primenjuju aplikacije
- Informacije o ažuriranjima koja su zamenila neka druga ažuriranja
- Brojeve predmeta povezanih sa Microsoftovom bazom znanja

## Korišćenje skenera za otkrivanje ranjivosti (vulnerability scanners)

Jedna od najdragocenijih metoda za proveravanje bezbednosti servera je korišćenje skenera za otkrivanje ranjivosti. Ovi skeneri se zasnivaju na konstantnom ažuriranju baze podataka o poznatim bezbednosnim pukotinama u operativnim sistemima i aplikacijama. Skener se spaja sa odredišnim sistemom na različitim portovima i šalje zahteve sistemu. Na osnovu odgovora, skener proverava bazu podataka da bi utvrdio da li postoje uslovi za neovlašćeno iskorišćavanje tog sistema. Svi potencijalni uslovi neovlašćenog korišćenja se sakupljaju u jedan izveštaj koji se prezentuje administratoru. Većina skenera ima opciju za nametljivo testiranje. Prilikom izvršavanja takvog testiranja je neophodna velika opreznost. Nametljivo testiranje je jedini način da zaista proverite rezultate testiranja ranjivosti. Na primer, u nekoj stavki izveštaja može stajati da je određeni skript preko web servisa označen kao izvršni i da se može iskoristiti tako da dovede do pada servera ukoliko prenese parametar koji sadrži nestandardni znak. Vi možete smatrati da to nije tačno, zato što ste dodelili NTFS dozvole skriptu da dopusti samo jednom nalogu da mu pristupi; taj nalog je onaj koji Vi kontrolišete i on nikada ne može da pošalje nestandardni znak. Jedini način da budete sigurni u to je da skener pokuša da iskoristi tu pukotinu u bezbednosti. Najbolje je da to uradite u toku održavanja, u slučaju da pokušaj skenera bude uspešan. Jedino nakon izvršavanja ovakve provere možete biti sigurni da ranjivost servera nije zaista prisutna.

Neki od poznatih skenera za otkrivanje ranjivosti su:

- Microsoft Security Baseline Analyzer
- Internet Security Systems: RealSecure
- Nessus
- GFI LANguard Network Security Scanner
- Cerberus Internet Scanner (CIS)

## Kontrolno praćenje fajl sistema

Windows 2003 poseduje ugrađene mehanizme za kontrolno praćenje pristupanja fajl sistemu. To Vam omogućava da vidite ko pristupa, ili pokušava da pristupi, određenim fajlovima i kada se to dešava. Ovu vrstu kontrolnog praćenja podržavaju samo diskovi sa NTFS-om. Da biste kontrolisali ovu vrstu pristupa, prvo morate da aktivirate Object Access Auditing. Ova osobina se aktivira preko Default Domain Security Settingsa, izabranjem Local Policies/Audit Policy/Audit Object Access. Kao što je prikazano na slici 1.5, potvrđite kontrolisanje obe opcije, Success i Failure, da biste pratili obe vrste događaja. Da biste kontrolisali pristup određenom fajlu ili direktorijumu, uradite sledeće:

### Upravljanje kontrolnim praćenjem na serveru

Uloga upravljanja kontrolnim praćenjem na serveru može biti dodeljena ne-administratorskom nalogu, garantovanjem Manage Auditing i Security Log prava preko Group Policy. Tako možete dodeliti ovu ulogu bez davanja punih administratorskih prava. To je posebno korisno za administratore udaljenih sajtova koji upravljaju samo podređenim skupovima servera i korisnika.

**Slika 1.5**

Postavljanje funkcije kontrolnog praćenja bezbednosti.



1. Preko Explorera pronađite fajl ili direktorijum.
2. Desnim tasterom miša kliknite fajl ili direktorijum koji će biti kontrolisani, kliknite Properties, a zatim Security.
3. Kliknite Advanced, a zatim kliknite dugme Auditing. Kliknite Add. Upišite naziv grupe ili korisnika čije akcije želite da pratite i kliknite OK.
4. U padajućem okviru Apply Onto izaberite lokaciju na kojoj želite da primenite kontrolno praćenje.
5. U okviru Access odredite koje uspešne i neuspešne događaje želite da kontrolišete, tako što ćete označiti odgovarajuća polja za potvrdu.
6. Kliknite OK, OK i OK da biste završili.

## Obezbeđivanje fajl sistema

Windows 2003 sve svoje podatke smešta u fajl sistem. Svi korisnički podaci, podaci aplikacije i fajlovi operativnog sistema nalaze se u fajl sistemu. Da bi Windows 2003 bio bezbedan, ovi fajlovi se moraju obezbediti. Spoljašnje pretnje mreži, slučajno brisanje fajl sistema ili pristup neke od neovlašćenih internih grupa mogu rezultirati gubitkom podataka ili ugrožavanjem poverljivih podataka. Windows 2003 podržava mnoge mehanizme za obezbeđivanje fajl sistema.

### Blokiranje fajl sistema preko NTFS-a

Još u Windowsu NT 3.1, Microsoft je uveo NT File System (NTFS). NTFS je predstavljao veliku prekretnicu u odnosu na FAT fajl sistem, u mnogim oblastima. Podržavanje većih diskova, podržavanje nestandardnih veličina bloka za dodeljivanje memorije i mogućnost definisanja bezbednosti na nivou fajla ili direktorijuma - sve su to velike prednosti NTFS-a u odnosu na FAT. Mogućnost obezbeđivanja pojedinačnih fajlova i direktorijuma preko NTFS dozvola predstavlja osnovu Windowsa 2003 kao bezbednog fajl servera.

Windows 2003 je napravio veliki korak napred u oblasti standardno podešenih sistemskih NTFS dozvola u fajl sistemu. Windows više ne podrazumeva postojanje grupe Everyone kojoj su se mogle dodeliti dozvole za sve resurse. Umesto toga, on podrazumeva dozvoljavanje mogućnosti identifikovanim korisnicima da čitaju i

prelistavaju fajlove i direktorijume. Po standardnom podešavanju, Windows 2003 će dozvoliti identifikovanim korisnicima da premoste poprečno proveravanje. To funkcioniše "ruku pod ruku" sa nadograđivanjem klijent operativnih sistema kao što su Windows 2000 Professional i Windows XP Professional koji sada dozvoljavaju mapiranje diskova na tački ispod pristupne tačke. Mada deljenje može da postoji u obliku \\Server\users\\$ sa direktorijumima odjeljenja i stotinama korisničkih direktorijuma ispod njih, korisnik sada može da bude mapiran u sopstvenom direktorijumu bez obaveze da eksplicitno deli korisnički direktorijum i bez obaveze da garantuje korisnička prava bilo čemu osim sopstvenom direktorijumu. Mada korisnik možda neće moći da čita ili prelistava direktorijume odjeljenja, to i nije neophodno ako je jedini cilj omogućiti korisniku pristup sopstvenom osnovnom direktorijumu. To će u velikoj meri pojednostaviti primenu NTFS dozvola.

## Blokiranje grupnog članstva

Jedan od najbitnijih načina za obezbeđivanje mreže je da se korisnicima ne garantuje članstvo u grupama koje bi im obezbedile više prava nego što im je zaista neophodno. Slično tome, ne sme se upasti u zamku proglašavanja svih administratora domena administratorima samo da biste bili sigurni da oni imaju "dovoljno" prava za izvršavanje dnevnih obaveza. Windows 2003 je nastavio da pravi velike korake unapred kada se došlo do dodeljivanja prava administratorima.

Oblast grupnog članstva, koju najčešće nadgledaju administratori, predstavljaju lokalne administrativne grupe na serverima članovima i radnim stanicama. Pošto za grupe ne postoji centralno upravljanje, veoma je lako zaboraviti da one uopšte postoje. Administratori obično dodaju korisničke naloge domena u svoje lokalne administratorske grupe, tako da korisnici mogu da rade na instaliranju novog softverskog paketa, ali često zaborave da uklone članstvo nakon završetka projekta. Rezultat toga je veliki broj korisnika koji imaju veća prava na njihovim radnim stanicama. Tako može da dođe do nesvesnog instaliranja špijunskih programa ili drugih aplikacija koje mogu da ugroze mrežu. Jedan od načina za kontrolisanje članstva lokalnih grupa je primena Group Policy Objectsa. Određivanjem grupe Administrators kao Restricted Group (zabranjene grupe), možete da odredite kojim nalozima je dozvoljeno da budu prisutni u toj grupi. Ako lokalni administrator unese dodatni nalog, ta izmena neće biti trajna. Ovaj parametar će pronaći u Computer Configuration/Windows Settings/Restricted Groups. Potrebno je samo da dodate grupu kojoj želite da zabranite pristup i dodate članstvo kojim je prisustvo dozvoljeno.

## Držanje korisnika dalje od sistemskih fajlova

Fajlovi operativnog sistema predstavljaju njegov krvotok. Korumpiranje ili brisanje ovih fajlova vrlo brzo može da onesposobi server. Ako ne računamo bezbednosne zakrpe, ne postoji nijedan drugi razlog da administrator ima pravo upisivanja za sistemske fajlove. Takva mogućnost bi samo učinila administratora pretnjom po stabilnost sistema. Slučajno brisanje fajlova ili njihovo preimenovanje kroz grešku operatora ili "zlonamerne" skriptove, može se sprečiti blokiranjem pristupa sistemskim fajlovima. Dozvolite nalogu Administrator da zadrži Full Control (potpunu kontrolu) nad fajlovima u direktorijumu %systemroot%, ali nemojte da dozvolite opštim administratorskim grupama da pristupaju ovim fajlovima. Nemojte da ohrabrujete administratore da se prijavljuju u sistemima kao Administrator. Umesto toga, ponudite im da koriste njihove regularne naloge i osobinu "ran as" ako je potrebno da pokrenu program koji zahteva veća prava.

## Obezbeđivanje web servisa

Web Servers su jedna od najčešćih implementacija Windowsa 2003 i zbog njihove funkcije da servisiraju korisnike izvan domena posebno su ranjivi i moraju biti dobro obezbeđeni. Nove zloupotrebe Weba se pojavljuju gotovo svakodnevno i da bi web serveri ostali bezbedni, moraju se ažurirati odgovarajućim zakrpama za operativni sistem, kao i za web servise.

### Korišćenje SSL-a

Ono o čemu treba najviše da brinete kada su u pitanju web serveri je kako da obezbedite poverljivu komunikaciju od presretanja. Pošto je Internet jedan "zamagljen oblak" sa diskutabilnom bezbednošću, samo od Vas zavisi kako će obezrediti end-to-end komunikaciju sa krajnjim korisnicima.

#### **Iskorišćenost propusnog opsega i SSL**

Korišćenje SSL-a ne utiče na iskorišćenost propusnog opsega. To, međutim, donosi dodatno opterećivanje CPU-a i klijenta i servera. Ako će postojeca web aplikacija biti prebačena na SSL komunikacije, ukupni kapacitet sistema će biti smanjen. To opterećivanje servera se može ublažiti upotrebom hardverskih SSL akceleratora.

Najjednostavnije je da to uradite pomoću Secure Socket Layer komunikacija. SSL se izvršava iznad TCP/IP-a, a ispod HTTP-a. SSL izvršava tri osnovne funkcije:

- **SSL autentifikaciju servera.** Ova funkcija omogućava klijentu da proveri identitet servera. Softver klijenta, sa aktivnim SSL-om, može da upotrebi kriptovanje javnim ključem i proveri da li su sertifikat servera i javni ID valjni. Isto tako, može da proveri da li je sertifikat objavljen od strane CA-a koji se nalazi u klijentovoj listi autoriteta za sertifikate u koje ima poverenja. Na primer, ako korisnik preko Interneta šalje broj kreditne kartice da bi nešto kupio, on će verovatno hteti da proveri identitet prijemnog servera.
- **SSL autentifikaciju klijenta.** Ova funkcija omogućava serveru da proveri identitet klijenta. Koristeći sličnu tehniku kao za autentifikaciju servera, softver servera, sa aktivnim SSL-om, može da proveri valjanost klijentovog sertifikata i javnog ID-a. Takođe, može da proveri da li je sertifikat objavio CA-a u koji ima poverenja. Na primer, ako online trgovac želi da pošalje kupcu poverljive informacije, on će verovatno hteti da proveri identitet tog kupca.
- **Šifrovanje SSL konekcija.** SSL zahteva da sve informacije koje se šalju između servera i klijenta budu šifrovane od strane softvera koji ih šalje i dešifrovane od strane prijemnog softvera. To omogućava visok nivo poverljivosti i bezbednosti. SSL sadrži mehanizam za pronalaženje podataka koje je neko neovlašćeno promenio. Sve naredne zaštićene transakcije se izvršavaju preko SSL konekcija.

### Skeniranja web servera radi otkrivanja ranjivosti

Web serveri su posebno ranjivi na napade hakera. Često su web serveri otvoreni za anonsne pristupe, a pritom nalaze se u slabo obezbeđenim mrežama. Web serveri su veoma popularne mete i zato se na web servisima uvek mogu pronaći slabe tačke.

Da biste eliminisali ranjivost sistema, morate da saznate njegove slabe tačke. Najjednostavniji način da to uradite je da redovno skenirate web servere tražeći gde su ranjivi.

Mnoge kompanije nude servise posebno dizajnirane za redovno skeniranje web servera, a svojim klijentima prosleđuju izveštaje o pronađenim slabostima. Ovo je odličan izbor za kompanije kojima nedostaju resursi ili stručnost za izvršavanje ovakvog unutrašnjeg skeniranja.

## Održavati korak sa zakrpama

Neprekidno održavanje koraka sa zakrpama je apsolutno neophodno za bezbednost web servera. Ogromna većina najbitnijih ispravki proizvedenih za Windows se zasniva na bezbednosnim pukotinama otkrivenim na web serverima. To se ne dešava zbog toga što su web serveri nepopravljivo nebezbedni, već zato što na Internetu postoji ogroman broj web servera zasnovanih na Windowsu; oni "nisu krivi" što predstavljaju omiljenu metu hakera. Microsoft ima čitave timove inženjera i softverskih dizajnera koji rešavaju takve probleme čim se pojave. Njihov posao je da brzo dostave administratorima najnovije ispravke. Najjednostavniji način za upravljanje ovim zakrpama je upotreba Software Update Servicea. SUS server omogućava usmeravanje svih web servera na jedan server radi preuzimanja zakrpa. Sve što treba da uradite je da proverite dnevниke zapisa na SUS serveru da biste videli da li ima novih zakrpa. Zakrpe možete da testirate u laboratorijskim uslovima, a zatim da odobrite njihovo dalje distribuiranje. Nakon toga, web serveri koji su konfigurisani tako da budu usmereni na SUS server, automatski će instalirati zakrpe i, opcionalno, ponovo pokrenuti sopstveni sistem.

### Zakrpe i automatsko restartovanje

Ako su serveri konfigurisani tako da automatski ponovo pokreću sistem nakon instaliranja zakrpa koje to zahtevaju, možete se naći u situaciji da se svi web serveri restartuju u isto vreme. Rezultat toga će biti da sajt neće raditi nekoliko minuta, u zavisnosti od toga koliko vremena je serverima potrebno da ponovo pokrenu sistem.

## Blokiranje IIS-a

Windows 2003 IIS (verzija 6.0) je nadmašio svog prethodnika u integriranju većine osobina starog IIS Lockdown Toola. IIS Lockdown Tool radi tako što isključuje nepotrebne osobine unutar IIS-a, na osnovu planirane uloge servera. Tako se smanjuje broj potencijalnih tačaka koje hakeri mogu da napadnu. Sve ovo je obloženo URLScanom, pomoćnim programom koji presreće ulaz sa računara klijenta i vrši internu proveru da bi utvrdio da li ima pokušaja slanja "zlonamernih" podataka kao što su znaci ili skriptovi koji izlaze iz dozvoljenog opsega. Po standardnom podešavanju, IIS6 se instalira samo sa onim osobinama koje su neophodne za obavljanje njegove definisane funkcije. Moguće je precizno odrediti koje ISAPI i CGI kodove je dozvoljeno pokrenuti na serveru, a postoje i standardno podešena ponašanja za upravljanje HTTP zagлавljima koja su dizajnirana za izvršavanje Web DAV-a. To zamenjuje neke od osobina URLScana. IIS6 sadrži i mehanizme za ograničavanje dužine polja i zahteva. Na ovaj način su prevaziđene gotovo sve slabosti starije verzije IIS-a. Ako su ovakva podešavanja suviše restriktivna za određenu web aplikaciju, možete da izmenite parametre preko podešavanja Registry:

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters\AllowRestrictedChars

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters\MaxFieldLength
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters\UrlSegmentMaxLength
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters\UrlSegmentMaxCount

Mada se URLScan 2.5 može izvršavati na IIS-u 6, većina administratora će zaključiti da to nije potrebno, zato što su osobine IIS-a 6, koje se tiču bezbednosti, bolje od onih u URLScanu 2.5. Preporučujemo da URLScan 2.5 koristite sa starijim IIS 5.0 serverima.

## Održavanje tajnosti fajlova pomoću EFS-a

Windows 2003 podržava Encrypting File System na NTFS volumenima. EFS omogućava korisniku da šifruje fajl tako da samo on može da mu pristupi. Kada počne da koristi EFS za šifrovanje fajla, korisniku se dodeljuje par ključeva (javni i privatni ključ). Ključevi se generišu pomoću servisa sertifikata ili ih EFS samostalno potpisuje, u zavisnosti od toga da li je CA prisutan. Javni ključ se koristi za šifrovanje, a privatni ključ za dešifrovanje.

Kada korisnik šifruje fajl, fajlu se dodeljuje slučajni broj, pod nazivom File Encryption Key (FEK). Za šifrovanje fajla se koristi DES ili DESX algoritam sa FEK-om kao tajnim ključem. FEK se, takođe, šifruje pomoću javnog ključa, koristeći RSA algoritam. Na ovaj način se veliki fajl može šifrovati korišćenjem relativno brzog kriptovanja tajnim ključem, dok se FEK šifruje sporijim, ali bezbednijim kriptovanjem javnim ključem. Tako se obezbeđuje visok nivo bezbednosti, sa manjim uticajem na sve ostale preformanse.

## Samostalna upotreba EFS-a

Windows 2000, 2003 i XP podržavaju EFS. Oni imaju sposobnost da generišu sopstveni par ključeva za EFS ukoliko nemaju na raspolaganju sertifikat na nivou domena. EFS na mašini koja ne pripada domenu se dosta razlikuje od onog na mašini koja je član domena. Na primer, Windows 2000 ima standardno podešen parametar koji dozvoljava svakom lokalnom nalogu Administrator da dešifruje svaki šifrovan fajl korisnika na toj mašini. To računare čini veoma ranjivim na napade, jer lokalni spremnik lozinke može biti ugrožen. Windows XP i Windows Server 2003 nemaju ovo ponašanje.

Ako korisnik šifruje fajl i izgubi oba spremišta sertifikata, korisničkog i lokalnog DRA-a, neće moći da dešifruje fajl. Slično tome, usled nedostatka centralne baze podataka ključeva za korisnike EFS-a na računaru koji ne pripada domenu, korisnik može namerno da izbriše DRA sertifikat i spremište sertifikata, pa će takvi fajlovi biti neupotrebљivi.

Kada koristite EFS u okruženju izvan aktivnog direktorijuma, možete da primenite neke od najboljih načina za upravljanje ključem i unapređivanje lokalne bezbednosti:

- Kod računara Windows 2000, standardno podešen DRA privatni ključ se mora ukloniti i smestiti odvojeno od sistema.

- Koristite SYSKEY mod sa diskete za podizanje sistema ili glavnu lozinku, koja se mora uneti pre podizanja sistema. Disketa ili glavna lozinka se moraju smestiti odvojeno od sistema. Tako ćete zaštiti lokalno spremište naloga od napada.

### Šifrovani fajlovi i standardno podešen domenski agent za opravak

Ako računar, ili korisnik, koji koriste samostalni EFS predu u pomoću CA-a predužeća, klijenti će nastaviti da koriste samostalno potpisane sertifikate. Oni se neće automatski registrovati za novi sertifikat čim se pridruže ovom okruženju. Međutim, standardno podešen domenski agent za opravak će uticati na sve nove fajlove. Postojeći šifrovani fajlovi će koristiti standardno podešen domenski agent za opravak nakon modifikovanja.

- Koristite Sysprep i ubičajene skriptove za konfiguriranje centralnog agenta za oporavak. To ćete uraditi preko pokretanja ključa Registrya koji uklanja postojeći lokalni DRA i postavlja centralizovan DRA. Ova promena se mora izvršiti nakon mini-podešavanja Sysprepa, koji generiše standardno podešen DRA. Najbolje je da koristite Microsoft CA za izdavanje DRA sertifikata za centralni agent za oporavak.

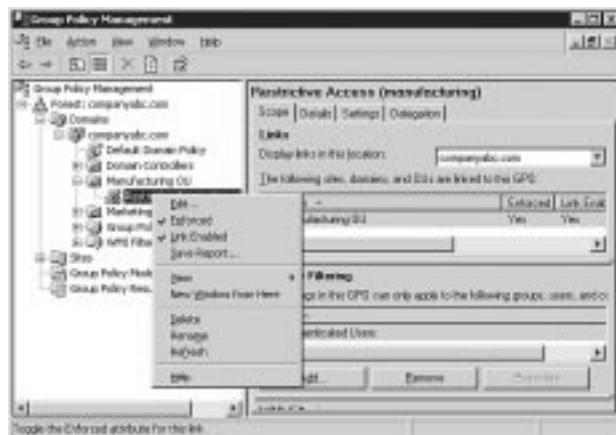
## Najčešće zamke u implementaciji Encrypted File Systema

Jedna od zamki Encrypted File Systema (EFS) u koju je najlakše upasti je da dozvolite korisnicima aktiviranje EFS-a na njihovim računarama, a bez pristupa domenskom agentu za oporavak. Klijenti će napraviti sopstveni par ključeva, a administratori možda neće moći da rekonstruišu šifrovane fajlove ako korisnik izgubi par lokalnih ključeva. Aktivni direktorijum omogućava da sprečite korisnike da aktiviraju EFS, sve dok odgovarajući CA ne bude postavljen tako da omogući upravljanje EFS-om na klijentima. Najjednostavniji način da to uradite je preko GPMC-a:

1. Otvorite Group Policy Management Console MMC.
2. Pronađite odgovarajući kontejner na koji će GPO biti primenjen.
3. Desnim tasterom miša kliknite GPO i označite Edit, kao što je prikazano na slici 1.6.

**Slika 1.6**

Editovanje GPO-a u Group Policy Management Console.



4. Prođite kroz \Computer Configuration\Windows Settings\Security Settings\Public Key Policies.
5. Desnim tasterom miša kliknite direktorijum pod imenom Encrypting File System.
6. Kliknite Properties.
7. Poništite potvrdu polja Allow Users to Encrypt Files Use Encrypting File System.
8. Kliknite OK.

## Neprobojni scenario

Kompanija ABC je mala softverska kompanija sa kancelarijama širom sveta. Ona se oslanja na trgovačke putnike koji putuju od kancelarije do kancelarije i ponosi se svojom sposobnošću da resurse stavi na raspolaganje krajnjim korisnicima. Kompanija ABC ima bezbednosna pravila koja zahtevaju šifrovanje svih podataka u bazama podataka i fajl serverima, kao i svih komunikacija između računara. Ona zahteva rigoroznu proveru identiteta za pristupanje svakom sistemu.

Bob je službenik kompanije ABC. On često radi kao trgovacki putnik. Njemu je potreban gotovo neprekidan pristup bazama podataka i elektronskoj pošti, pa zato ima nov, moderan prenosivi računar za bežičnom mrežnim interfejsom i Windowsom XP.

U ovom odeljku će biti opisan Bobov tipičan radni dan i one karakteristike koje Bobu omogućavaju da izvršava svoje dnevne zadatke na bezbedan način.

Bob je upravo stigao u udaljenu kancelariju i potrebno mu je da pristupi dokumentu koji je smestio na fajl serveru u centrali kompanije. Dodeljena mu je sala za konferencije da je koristi kao svoju privremenu kancelariju. Bob pokreće sistem na svom prenosivom računaru, koji ga "pita" da li želi da unese svoju inteligentnu karticu. On smešta svoju propusnicu u čitač inteligentne kartice i sada se od njega traži PIN. Bob upisuje PIN i tako potvrđuje identitet. Čim prenosivi računar pokrene Windows XP, sistem šalje DHCP zahtev preko bežične mreže. Zajedno sa DHCP zahtevom, Bobov sistem šalje i ClassID koji je konfigurisan u sistemu. Srećom po Bobu, MAC adresa njegove bežične kartice je uneta u RADIUS server, koji koristi sve tačke bežičnog pristupa za proveru identiteta korisnika na hardverskom nivou. To omogućava tački pristupa da obradi Bobov DHCP zahtev. Zahtev dospeva do DHCP servera koji je smešten na izdvojenoj mreži u kancelariji. Ova mreža se nalazi iza zaštitnog zida i dozvoljava samo VPN saobraćaju da dođe do određenog para VPN servera. Pošto se ClassID na Bobovom računaru poklapa sa ClassID-om na DHCP serveru, Bobovom računaru se daje validna IP adresa.

Bob pokreće VPN konekciju i spaja se sa lokalnim VPN serverom. Bob sada ima L2TP konekciju, obezbeđenu pomoću IPSeca, sa kancelarijskom mrežom. Na ovoj tački se pojavljuje zahtev za unos prijave domenu i Bob potvrđuje svoj identitet mreži preko svoje prijave u aktivnom direktorijumu. Zadovoljan svojim napredovanjem, Bob odlučuje da nagradi sebe šoljom fine kafe. Pošto zna da mora da ima propusnicu da bi ušao u kuhinju, Bob izvlači propusnicu iz prenosivog računara i odlazi u kuhinju. Nakon uklanjanja propusnice, drajver inteligentne kartice "saopštava" sistemu da se zaključa.

Ovo ponašanje je konfigurisano u prenosivom računaru. Dok Bob nije tu, ostali korisnici ne mogu da pristupe njegovom prenosivom računaru. Bob se ubrzo vraća i otključava svoj prenosivi računar pomoću inteligentne kartice i PIN-a. Pošto Bob ima pristup korporacijskoj mreži, on odlučuje da pristupi svom dokumentu na serveru u centralni kompanije.

Kada Bobov računar zatraži fajl od servera, server će ga informisati da zahteva Transport Layer Security za pristupanje resursima. Bobov prenosivi računar i server će razmeniti sertifikate i slučajne vrednosti i tako stvoriti pre-master tajnu. Ova tajna se koristi za generisanje njihovih ključeva sesije. Ključevi sesije se koriste za šifrovanje komunikacija. Kada Bobov prenosivi računar "kaže" serveru koje šifre podržava, informisaće server da podržava samo Microsoft Enhanced DSS i Diffie-Hellman SChannel Cryptographic Provider, što predstavlja način na koji je prenosivi računar konfigurisan. Server prihvata ove šifre i kanal je uspostavljen.

Dokument koji je Bobu potreban se nalazi u njegovom ličnom direktorijumu. Ovaj direktorijum se šifruje preko EFS-a na osnovu sertifikata koji je Bobu izdao korporacijski autoritet za sertifikate. Pošto Bobov prenosivi računar poseduje ispravan ključ, on može da dešifruje fajl i prikaže ga. Bob je, takođe, ovlastio nekoliko saradnika da dešifruju fajl, tako da se fajl može deliti.

Bob zaključuje da je sve to, ipak, previše naporno da bi došao samo do jednog fajla. Pošto zna da će ovom fajlu morati da pristupi i sutra u sledećoj kancelariji, Bob odlučuje da napravi lokalnu keširanu kopiju fajla kroz offline direktorijume. Na sreću, Windows XP klijent, sa Windowsom 2003 na drugom kraju, dozvoljava Bobovim offline kopijama da ostanu šifrovane. Kada Bob ponovo izgubi prenosivi računar na aerodromu, kompanija neće morati da brine o gubitku intelektualne svojine.

## Zaključak

U ovom poglavlju ste naučili da je Microsoft napravio velike korake unapred, čineći komunikacije i spremnike mnogo bezbednijim. Windows 2003 predstavlja najnoviji pokušaj Microsofta u ovoj oblasti. Uočili ste važnost slojevitog pristupa bezbednosti. Ni jedna pojedinačna tehnologija u Windowsu 2003 ne pokriva ukupnu bezbednost. Sve tehnologije funkcionišu zajedno kako bi pomogle u obezbeđivanju intelektualne svojine kompanije, lokalno i spolja.

Videli ste da je bezbednost sistema veoma važna, ali da je konstantno kontrolno praćenje i testiranje bezbednosti isto toliko važno. Nadgledanje aktivnosti na mreži i prepoznavanje simptoma napada su veoma važni za zaštitu mreže.

Tehnologije, kao što su inteligentne kartice i biometrija, pomažu ojačavanju procesa provere identiteta u Windowsu. Tehnologije, kakve su TLS i SSL, pomažu da budete sigurni da kada se identitet jednom proveri, svi prenosи nastavljaju da se izvršavaju na bezbedan način.

Fajlovi mogu da se šifruju, ali i dalje mogu da se dele u okviru kontrolisane liste korisnika. Smeštanjem šifrovanih fajlova, sistem postaje otporniji na krađu podataka i ako dođe do krađe hardvera. To omogućava kompanijama da dozvole slobodniji pristup podacima, a da to ne ugrozi ukupnu bezbednost okruženja.

Veoma je važno shvatiti da bezbednosni sistem koji se danas ne može "provaliti", sutra može da postane prava igračka. 128-bitno šifrovanje, koje je nekada zahtevalo godine rada da bi se razbile šifre, današnji moćni računari "razbijaju" za nekoliko sekundi. Bezbednost podrazumeva posvećivanje; to je proces koji se mora stalno nadgledati i održavati. Bezbednost mora da raste zajedno kompanijom da bi od nje uopšte bilo koristi.