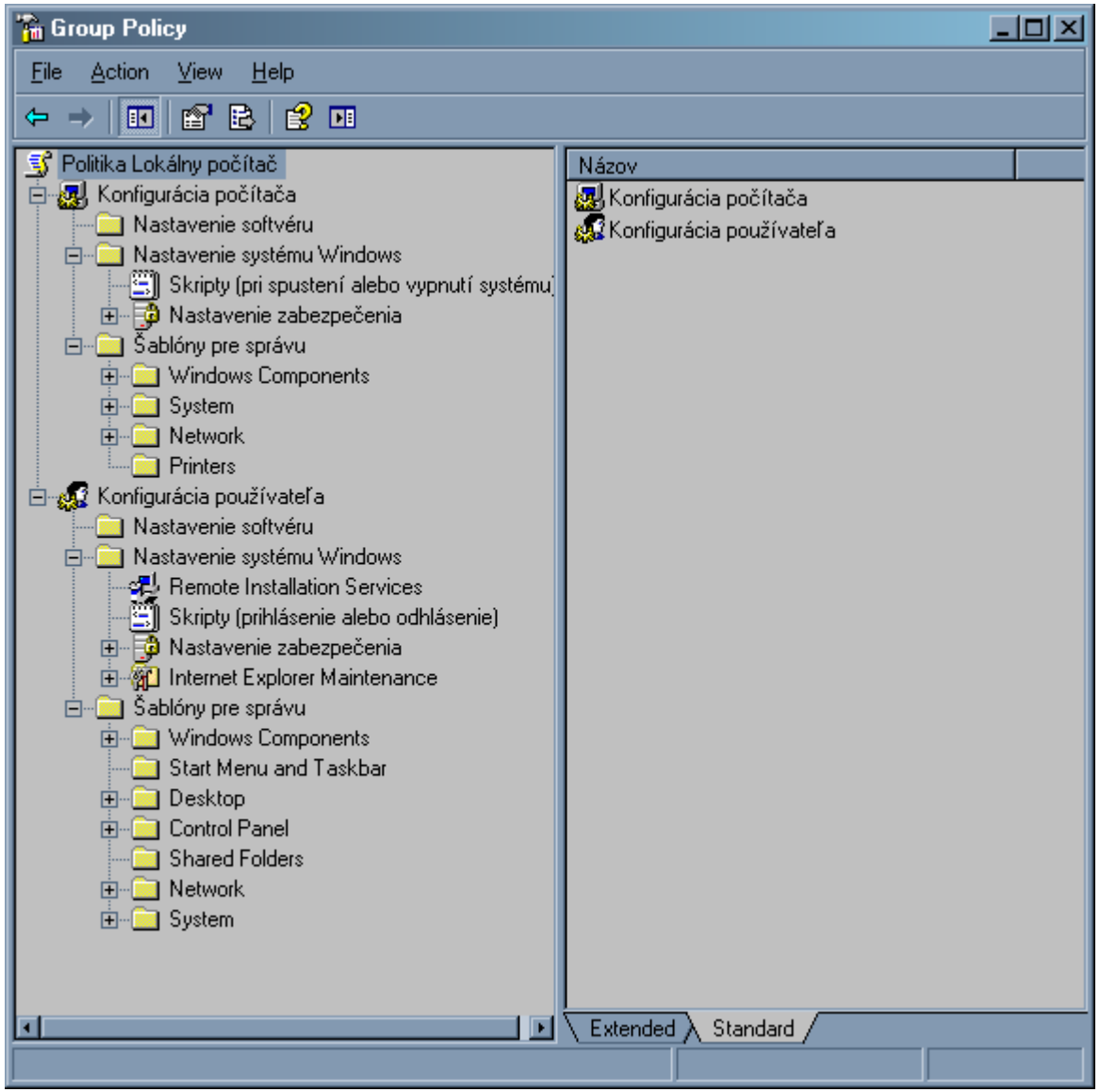
Odhodlal som sa napísať niekoľko rád, ako zlepšiť zabezpečenie počítača s operačným systémom z dielní MS. Je to možné viacerými spôsobmi, ale za najvhodnejší považujem použiť všeobecný editor politík, konkrétne "gpedit.msc". Je možné použiť aj nástroj "secpol.msc", ale ten sa nezaoberá tak rozsiahlymi politikami (viacmenej iba priamo zabezpečenie užívateľa a následnej správy, systémové politiky zahŕňa iba okrajovo), na rozdiel od "gpedit.msc".
CHel by som ešte poznamenať, že užívateľ, ak sa chce "pohrať" s nastavením systému za účelom či už zvýšenia bezpečnosti, alebo len tak skúsiť niečo nové, by mal aspoň ovládať tie najzákladnejšie úkony práce s počítačom (práca s myšou, klávesové skratky, základné znalosti o tom, ako funguje operačný systém MsWindows), poprípade, ak si niekde niečo zmení alebo prestaví, tak nech si to niekam napíše-zaeviduje, aby sa potom nemusel dožiť toho, že sa beh udalostí nebude vyvíjať želateľným smerom, v tom prípade bude šíriť paniku a bude počítač zbytočnými nadávkami a fyzickými útokmi (kopanie doň, búchanie po klávesnici a pod.) kompromitovať.
Článok je predovšetkým určený začiatočníkom, ktorý sa neboja experimentovať a zároveň su uvedomujú, že predvolené nastavenia systému sú nedostatočné vzhľadom na dnešné pomery. Niektoré súčasti som vynehal kvôli prílišnej kompexnosti-zložitsti, niektoré kvôli vysokej odbornosti a niektoré súčasti alebo vysvetlenia som značne zjednodušil pre principiálne pochopenie, tak ma prosím neukameňujte za to (profesionáli z oblasti IT bezpečnosti).
Prakticky veľkú časť mnou spomenutých nastavení budete môcť uplatniť, či už pred nezodpovednými užívateľmi, alebo útočníkmi, priamo snažiacimi sa dostať do Vášho systému za účelom Vám uškodiť, alebo spôsobiť stratu / odcudzenie dát, alebo zmeniť niektoré zužívané funkcie. Je jasné, že dokonalý systém neexistuje a vždy sa dá nájsť nejaký spôsob, ako sa dostať do systému, ale pomocou niektorých z týchto nastavení sa Váš systém stane rozhodne ťažším orieškom pre potencionálneho útočníka, ako bol po štandartnej inštalácii. Tu uvedené je aplikovateľné na operačné systémy: Windows2000proffesional-prac. stanica, Windows2000proffesional-server, WindowsXPproffesional, Windows2003-server, z určitými zmenamy a obmezdeniami aj WindowsVista, Windows7 a WindowsServer-2008. Žial MS neumožnil majiteľom systémov WindowsXP-HomeEdition využívanie tohto nástroja.
Pod správcovským účtom vykonáme nasledovné: štart, spustiť, napíšeme gpedit.msc a príkaz potvrdíme enterom či myškou. Pred nami sa objaví konzola všeobecných politík systému. Nebudem tu robiť kompletný súpis všetkých položiek, ale iba tých dôležitejších, pretože sa po prvé nepovažujem za naslovovzatého odborníka v oblasti zabezpečenia počítačových systémov a po druhé, možností je veľmi veľa a dal by sa o tom napísať seriál s takým počtom dielov, že by v pohode "utrel" aj sebelepšiu telenovelu :-).
Nástroj gpedit sa člení na dve základné kategórie, a to "Politika Lokálny Počítač" a "Konfigurácia Používateľa". V krátkosti zrhniem, prvá sa zaoberá prevažne nastavením systému a jeho zabezpečením a druhá sa dotýka práv užívateľských účtov, i keď sa niekedy navzájom zasahujú do kompetencií.

Poďme si niektoré z nich trochu ozrejmiť.
Hlavné okno je rozdelené na ľavú stromovú časť a pravú, položkovú. V ľavej časti okna je stromová vetviteľná štruktúra, ktorou sa budeme riadiť (znamienkami "+" otvárame stromovú štruktúru a znamienkami "-" ju opačne uzatvárame) a v pravej položková - údajová časť.



Poďme sa venovať prvej hlavnej vetve politík nástroja "gpedit.msc".

Politika Lokálny Počítač - Konfigurácia Počítača - Nastavenie Systému Windows - Nastavenie Zabezpečenia - Politiky Konta - Politika Hesla

Heslo musí spĺňať požiadavky na zložitosť (Password must meet complexity requirements).
Sú dve možnosti, politika je povolená, či zakázaná. Ak ju povolíme, pri založení akéhokoľvek účtu, alebo zmene hesla už existujúcemu účtu, bude systém od nás požadovať splnenie niekoľkých požiadaviek súčasne a to konkrétne: heslo nesmie obsahovať názov užívateľského účtu, či i len časť jeho plného názvu. Ďalej je požiadavka na minimálny počet znakov, teda minimálne 6 znakov, alebo viacej. Ďalej je požiadavka na splnenie troch požiadaviek zo štyroch, a to:

1. **kapitálky, teda veľké znaky (A-Z)**
2. **malé znaky (a-z)**
3. **základné číslice (0-9)**
4. **aspoň jeden zo špeciálnych (neabecedných a nenumerických) znakov (napríklad znamienko plus, alebo mriežka či lomítko a pod.)**

maximálna doba platnosti hesla (Maximum password age)
Hádam netreba veľmi vysvetľovať, je jasné, že sa tu jedná o nastavenia času, dokiaľ nevyprší platnosť hesla účtu. Možnosti sú od 1 až po 999 dní (teda od jedného dňa po zhruba dva a trištvrte roka), alebo je možnosť nastavením na 0 úplne potlačiť časové obmedzenie a heslo bude platné stále, až do vykonania priamej zmeny vyvolanej užívateľom, alebo správcom systému

minimálna dĺžka hesla (Minimum password length)
nám zaručí, že v hesle nesmie byť menší počet znakov, ako je nastavené politikou. Možností sú od 0, teda prakticky účet môže byť bez hesla, až po počet znakov 14, čo už zabezpečí slušnú ochranu proti útokom typu BruteForce (útok hrubou silou). Samozrejme, nik Vám nebude brániť urobiť si paranoja heslo hoci aj s počtom znakov 100, otázkou však ostane, či by si také heslo vôbec niekto pamätal, predpokladám, že asi len filmový hrdina typu RainMan :-)))

minimálna doba platnosti Hesla (Minimum password age)
asi netreba obšírne písať, v krátkosti, jedná sa o minimálny čas, pokiaľ heslo účtu ostáva v platnosti. Je jasné, že údaj tejto položky musí byť menší minimálne o jeden deň, ako údaj v položke Maximálna Doba Platnosti Hesla

vynútiť použitie histórie hesiel (Enforce password history)

nám zabezpečí, aby sa nemohlo heslo opakovať aspoň toľko krát, koľko bude nastavené politikou. Teda konkretizujme. Ak nastavím napríklad na 3, nesmie sa opakovať rovnaké heslo do troch zmien, ináč povedané, rovnaké heslo sa smie použiť až na štvrtý krát, dovtedy vždy iné

Politika Lokálny Počítač - Konfigurácia Počítača - Nastavenie Systému Windows - Nastavenie Zabezpečenia - Politiky Konta - Politika Uzamknutia Konta

hraničná hodnota uzamknutia konta (Account lockout threshold)
nám zabezpečí, že po prekročení daného limitu počtou pokusov o neúspešné prihlásenie sa k účtu sa nám účet uzamkne na stanovenú dobu, čas sa upresní v nasledujúcej politike

trvanie uzamknutia konta (Account lockout duration)
nám zabezpečí, že sa užívateľ až do uplynutia stanoveného času nebude môcť prihlásiť na svoj účet napriek tomu, že bude dávať správne heslo (pretože je prekročený limit pokusov na prihlásenie sa a tým sme si svoj účet uzamkli)

vynulovať počítadlo uzamknutia konta po čase (Reset account lockout counter after)
zabezpečí, že po politikou uplynutom čase sa znova môžme pokúsiť prihlásiť sa na účet bez toho, aby sme si ho znovu zablokovali, pokiaľ neprekročíme maximálny počet pokusov o prihlásenie sa určenom hraničnou hodnotou uzamknutia konta, pre pochopenie uvediem príklad. Hraničná hodnota uzamknutia konta je nastavená na 10 neúspešných prihlásení sa k účtu a politika "trvanie uzamknutia konta" je nastavená na 30 minút, politika "vynulovať počítadlo uzamknutia konta po čase" je nastavená na 15 minút. Ak si zablokujem účet prekročením limitu pokusov o prihlásenia sa, mám síce účet uzamknutý na pol hodinu, ale po 15 minútach sa mi "vynuluje" čítač neúspešných pokusov, ktorý spôsobí, že znova mám možnosť 10 krát sa pokúsiť o prihlásenie sa, kým sa mi znova neuzamkne účet, teda sa buď prihlásim správnym heslom, alebo sa mi posunie automatické odomknutie účtu o ďaľšiu polhodinu

Politika Lokálny Počítač - Konfigurácia Počítača - Nastavenie Systému Windows - Nastavenie Zabezpečenia - Lokálne politiky - Politiky Auditu

zabezpečujú auditovanie (sledovanie) procesov transakcií a udalostí, dejúcich sa v systéme. Tu sú niektoré z nich bližšie popísané:

Použitie oprávnení

Toto sledovanie umožňuje zistiť, či niekto vykonáva úlohu v počítači, na ktorú má povolenie

Prístup k adresárovým službám
Sledovanie umožňuje zistiť, či niekto získal prístup k objektu služby Active Directory s vlastným zoznamom systémových prístupových práv

Prístup k objektom
Sledovanie umožňuje zistiť, či niekto použil súbor, priečinok, tlačiareň alebo iný objekt. Taktiež môžete auditovať kľúče databázy Registry, čo neodporúčame, pokiaľ nemáte pokročilé počítačové znalosti a nepoznáte spôsob používania databázy Registry

Sledovanie procesov
Toto sledovanie umožňuje zistiť udalosti, ako je napríklad aktivácia programu alebo ukončenie procesu

Správa konta
Sledovanie umožňuje zistiť, či sa zmenil názov konta, či sa konto aktivovalo alebo deaktivovalo, vytvorilo alebo zrušilo, či sa zmenilo heslo, alebo či sa zmenila používateľská skupina

Systémové udalosti
Sledovanie umožňuje zistiť, ak niekto vypol alebo reštartoval počítač, alebo ak sa program pokúša vykonať niečo neoprávnené. Ak sa napríklad spyware pokúsil zmeniť nastavenie počítača bez vášho povolenia, sledovanie systémových udalostí to zaznamená

Udalosti prihlásenia
Sledovanie umožňuje zistiť, ak sa niekto prihlásil do počítača alebo z neho odhlásil (buď priamo v počítači alebo prostredníctvom prihlásenia cez sieť)

Zmena politiky
Sledovanie umožňuje zistiť pokusy o zmenu lokálnych politík zabezpečenia a zistiť, či sa zmenili priradenia používateľských práv, politiky auditovania alebo politiky dôveryhodnosti

Politika Lokálny Počítač - Konfigurácia Počítača - Nastavenie Systému Windows - Nastavenie Zabezpečenia - Lokálne politiky - Priradenie Práv Používateľov

Spomeniem iba niektoré položky, ostatné sú veľmi špecifické, vhodné iba pre správcov systémov a sietí ActiveDirectory, v domácom prostredí ťažko nájdu uplatnenie.

Force shutdown from a remote system
zabezpečí, že používateľ alebo skupina používateľov, má právo na diaľku (po sieti) počítač vypnúť, resp. ho reštartovať

Change the system time
zabezpečí, že používateľ alebo skupina používateľov, má právo nastavovať-meniť systémový čas počítača

Increase scheduling priority
zabezpečí, že používateľ alebo skupina používateľov má právo meniť prioritu behu programov (typicky cez TaskManager - "taskmgr.exe" - starý dobrý správca úloh systému windows)

Load and unload device drivers
zabezpečí, že používateľ alebo skupina používateľov, má právo inštalovať, odoberať alebo vymienať ovládače zariadení (typicky napríklad tlačiareň, klávesnica, myš, skener a pod.)

Modify firmware environment values
zabezpečí, že používateľ alebo skupina používateľov, má právo modifikovať FirmWare (zjednodušene a laicky povedané, primárny systémový program, ktorý je obsiahnutý v NVRAM, akým je napríkald BIOS počítača, IP kamery, sieťového rútru a pod.)

Deny log on through Terminal Services
zabezpečí, že používateľ alebo skupina používateľov, má alebo nemá právo sa prihlásiť prostrednictvom terminálových služieb (dobre známa Vzdialená pracovná Plocha/RDP - "mstsc.exe" či "tsmmc.msc")

odoprieť lokálne prihlásenie (Deny log on locally)
zabezpečí, že používateľ alebo skupina používateľov, má alebo nemá právo sa prihlásiť svojím účtom do počítača

odoprieť prístup na tento počítač zo siete (Deny access to this computer from the network)
asi netreba obzvlášť vysvetlovať, používateľ alebo skupina používateľov nemá právo na prístup do počítača zo siete (typicky napríkald po zdieľaní)

prihlásiť sa lokálne (Allow log on locally)
asi tiež netreba obzvlášť vysvetlovať, používateľ alebo skupina používateľov má právo sa prihlásiť lokálne na počítač (ak pridáme skupinu/užívateľa, nezávisle na tom, aké je nastavenie cez správcu užívateľov, zabezpečíme možnosť prihlásenia sa, ak sú splnené ďalšie podmienky {účet nie je zablokovaný, účtu nevypršala expirácia a pod.}). Túto konkrétnu politiku treba používať veľmi opatrne a radšej robiť klasickú správu užívateľov, sám MS tvrdí, že zmeny nastavenia môžu mať neblahý dopad na kompatibilitu niektorých klientov, služieb a aplikácií

prístup k počítaču zo siete (Access this computer from the network)
používateľ alebo skupina používateľov má právo prístupu po sieti, pozor, je to nezávislé na prístupe cez RDP ("mstsc.exe", "tsmmc.msc"), teda terminálové služby nie sú touto politikou postihované

Restore files and directories
zjednodušene povedané, používateľ alebo skupina používateľov má právo prístupu k obnove dát zo záloh a záložných médií či iných zdrojov predvolene majú na to právo iba skupiny Backup Operators alebo Administrators a ich členovia).

Shut down the system
netreba obzvlášť vysvetlovať, používateľ alebo skupina používateľov má právo vypnúť/reštartovať počítač (pozn. na WinServer je prednastavené povolenie vypnúť systém iba skupina Administrators, na Win2000/WinXP/Winvista/Win7 {prakticky každému, ešte pred prihláseím sa k účtu užívateľa})

Politika Lokálny Počítač - Konfigurácia Počítača - Nastavenie Systému Windows - Nastavenie Zabezpečenia - Lokálne politiky - Možnosti Zabezpečenia

Accounts: Limit local account use of blank passwords to console logon only
politika povoľuje / zakazuje prihlásiť sa účtom bez hesla, (platí iba pre lokálne prihlásenie, nie sieťové - RDP{"tsmmc.msc", "mstsc.exe"})

Audit: Shut down system immediately if unable to log security audits
zabezpečí, že ak sú naplnené auditovacie LOG súbory (jednotlivé položky v denníku udalostí / "eventvwr.msc"), s tým, že je nastavené manuálne čistenie LOG súborov, počítač sa vypne. Používať veľmi opatrne, v prípade, že nie je auditovanie nastavené na automatické čistenie LOG súborov po zaplnení, príde hláška:

"STOP: C0000244 {Audit Failed}
An attempt to generate a security audit failed."

a počítač sa vypne !!! Jedine členovia skupiny administrators sú výnimkou a dostanú sa do systému, kde je ale odporúčané zmeniť nastavenie auditovania (Zobrazovač Udalostí - "eventvwr.msc" u konkrétnych položiek {Application, Security, System, ...} a nastaviť dostatočne veľkú veľkosť denníka {zo skúseností dávam aspoň 4096 kB} a nastaviť prepisovanie udalostí podľa potreby - obzvlášť u WindowsServer2003 sa to môže vyskytnúť

(v závislosti aj na iných nastaveniach, nie len cez politiky), v každom prípade odporúčam skontrolovať - nastaviť a nešetriť miestom, čím je LOG súbor väčší, o to bude dlhšií časový záznam-história)

Devices: Allowed to format and eject removable media
politika povoľuje užívateľom / skupinám v zozname formátovať a vysúvať vymeniteľné médiá (USB kľúče, cd/dvd RW/RAM, diskety, páskové knižnice a pod.)

Devices: Prevent users from installing printer drivers
politika zakazuje užívateľom / skupinám v zozname inštalovať / odoberať ovládače tlačiarní

Devices: Restrict CD-ROM access to locally logged-on user only
politika zakazuje užívateľom / skupinám v zozname prístup na jednotku CD/DVD (lokálne aj po sieti)

Devices: Restrict floppy access to locally logged-on user only
politika zakazuje užívateľom / skupinám v zozname prístup na jednotku FDD (disketová jednotka)

Devices: Unsigned driver installation behavior
politika určuje, ako sa má chovať inštalátor počas inštalácie nepodpísaných ovládačov.Sú tri možnosti:
1. silently succeed / voľný preklad - tichý súhlas, teda nainštaluje za každých okolností
2. warm but allow installation / nainštaluje sa, ale pokiaľ nespĺňa podmienky podpisu, príde o tom výstraha
3. do not installation / inštalácia nepodpísaného ovládača nebude možná

interactive logon: Display user information when session is locked
určuje, aká sá má zobraziť informácia počas uzamknutia počítača (WinKey + L)

Interactive logon: Do not display last user name
určuje, či sa nemá alebo má zobraziť účet posledného prihláseného užívateľa (platí iba pri lokálnom prihlásení, nemá to vplyv na RDP)

Interactive logon: Do not require CTRL+ALT+DEL
politika povoľuje alebo zakazuje požiadavku na stlačenie slávneho trojhmatu CTRL+ALT+DEL za účelom prihlásenia sa do systému (platí iba pri lokálnom prihlásení, nemá to vplyv na RDP)

Interactive logon: Message text for users attempting to log on

týmto sa vyplní hlavička textu správy pre užívateľa, ktorý sa bude prihlasovať

Interactive logon: Message title for users attempting to log on
týmto sa vyplní samotný text správy pre užívateľa, ktorý sa bude prihlasovať

Kontá: premenovať konto Administrator (Accounts: Rename administrator account)
spôsobí zmenu názvu vstavaného účtu ADMINISTRATOR (odporúčam zmeniť, utočník prepokladá existenciu účtu a to, že je štandartne neblokovaný a ešte lepšie je účet zakázať, bude spomenuté nižšie)

Kontá: premenovať konto Guest (Accounts: Rename guest account)
spôsobí zmenu názvu vstavaného účtu GUEST, spôsobí zmenu názvu vstavaného účtu (odporúčam zmeniť, utočník prepokladá existenciu účtu a to, že je štandartne neblokovaný a ešte lepšie je účet zakázať, bude spomenuté nižšie)

Kontá: stav konta Administrator (Accounts: Administrator account status)
nastavenie povolí alebo zakáže účet, vrelo odporúčam zakázať, pochopiteľne, ešte pred samotným zakázaním vstavaného účtu si založíme nový správcovský účet

Kontá: stav konta Guest (Accounts: Guest account status)
nastavenie povolí alebo zakáže účet, vrelo odporúčam zakázať, nevidím veľký význam v používaní tohoto účtu, nie je predsa žiadny problém si založiť akýkoľvek iný účet s s adekvátnymi (najnižšími) právami

Network security: Do not store LAN Manager hash value on next password change
zakáže alebo povolí ukladenie LM hashu (veľmi zjednodušene a laicky povedané, je to chránený zoznam účtov a hesiel), uložený predvolene na disku pevného počítača (ale jestvuje aj možnosť ukadať na disketu, či iné médium). Vo WinVista/Win7 je predvolene povolené, teda sa hash neukladá, ale v starších systémoch, ako Win2000 či WinXP veľmi dôrazne odporúčam rozhodne zmeniť, teda zakázať ukladanie hešu na disk, to sťaží útočníkoví útok na Váš počítač, spolu s inými bezp. nastaveniami. HASH býva často vďačným objektom útočníkov, a preto ak si aspoň trochu ceníte svoje dáta, treba povoliť politiku. Ešte by som dodal, pre úplné uplatnenie politiky odporúčam vykonať reštart počítača a znova si pomeniť heslá, hoci aj na také isté (ide o to, aby už neboli ukladané v "staršom formáte" (LM-hash))

konzola po zotavení: povolenie automatického správcovského prihlásenia (Recovery console: Allow automatic administrative logon)

povolí, alebo zakáže automatické prihlásenie sa účtu Administrator v Núdzovom Režime (upozornenie! aj napriek tomu, že bude politikami alebo priamo cez správcu užívateľov účet Administrator zablokovaný, v Núdz. Režime a v konzole po zotavení bude stále prístupný a v konzole po zotavení sa bude iba tento výhradne používať !!! Aj preto odporúčam na už zakázaný účet Administrator nastaviť "silné heslo"). Je to ďalší vďačný spôsob pre útočníka, ktorý ak by sa dostal fyzicky k Vášmu počítaču, resetne počítač, a cez Núdz. Režim alebo konzolu po zotavení by teoreticky mohol mať prístup do Vášho systému. Teda jednoznačne zakázať!!!

Recovery console: Allow floppy copy and access to all drives and all folders
politika povoľuje alebo zakazuje kopírovať z diskety a mať prístup k jednotkám, ako aj súborom a adresárom. Podľa mňa čiastočne kontraproduktívne, ale pre zabezpečenie počítača je politikou dobré mať nastavenie na zákaz, ale povedzme si úprimne, Núdz. Režim a konzolu po zotavení spravidla potrebujeme, keď riešime vážny problém so systémom, kde by nám ale takéto nastavenie zbytočne komplikovalo prácu, ba až znemožnilo. Je iba na Vás, ako si nastavíte túto položku

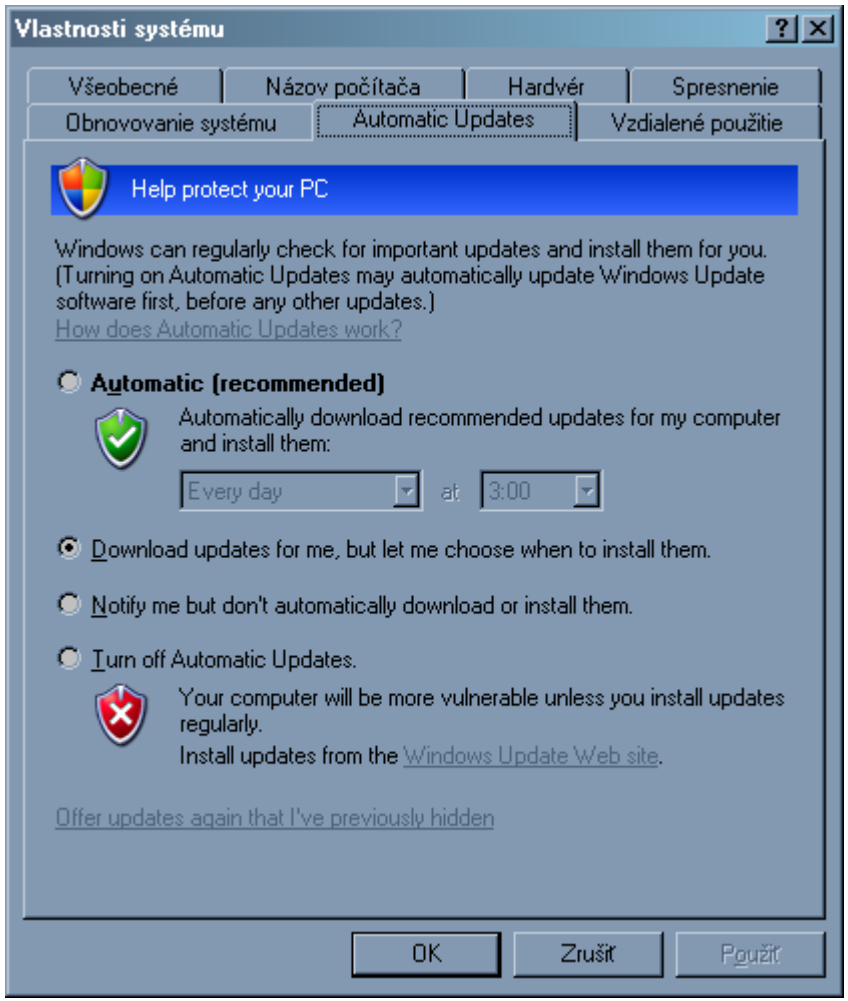
Shutdown: Allow system to be shut down without having to log on
politika povolí, alebo zakáže vypnutie počítača bez nutnosti prihlásenia sa do počítača akýmkoľvek účtom. Odorúčam vypnúť iba na počítači, ktorý bude v pozícii servera (Win 2000, WinXP (FileServer, Printserver, TerminalServer a pod.)) pri Win2003server a Win2008server je to už samozrejme impicitne zakázané.

Shutdown: Clear virtual memory pagefile
politika povolí, alebo zakáže vyčistenie stránkovacieho súboru počas vypínania / reštartu počítača. Ďalšia potencionálna hrozba, ak napríklad používate na lokálnom počítači viacej ako jeden OS, v momente, ak je jeden z OS neaktívny, je možnosť, že sa dostane k dátam uchovaných vo SWAP súbore neaktívneho OS niekto, kto by ich vedel aj dobre využiť(alebo ak sa útočník dostane k Vášmu vypnutému počítaču {ale to by už ani čistenie SWAP-u pochopiteľne nepomohlo}). Hlavne vo firmách odporúčam povoliť, počítač sa zriedkakedy púšťa viacej ako jeden krát za pracovný deň a vypínanie na fajront natiahnuté o dve či tri minútky určite nikoho nezabije a ani neskrachuje na účte za el. prúd

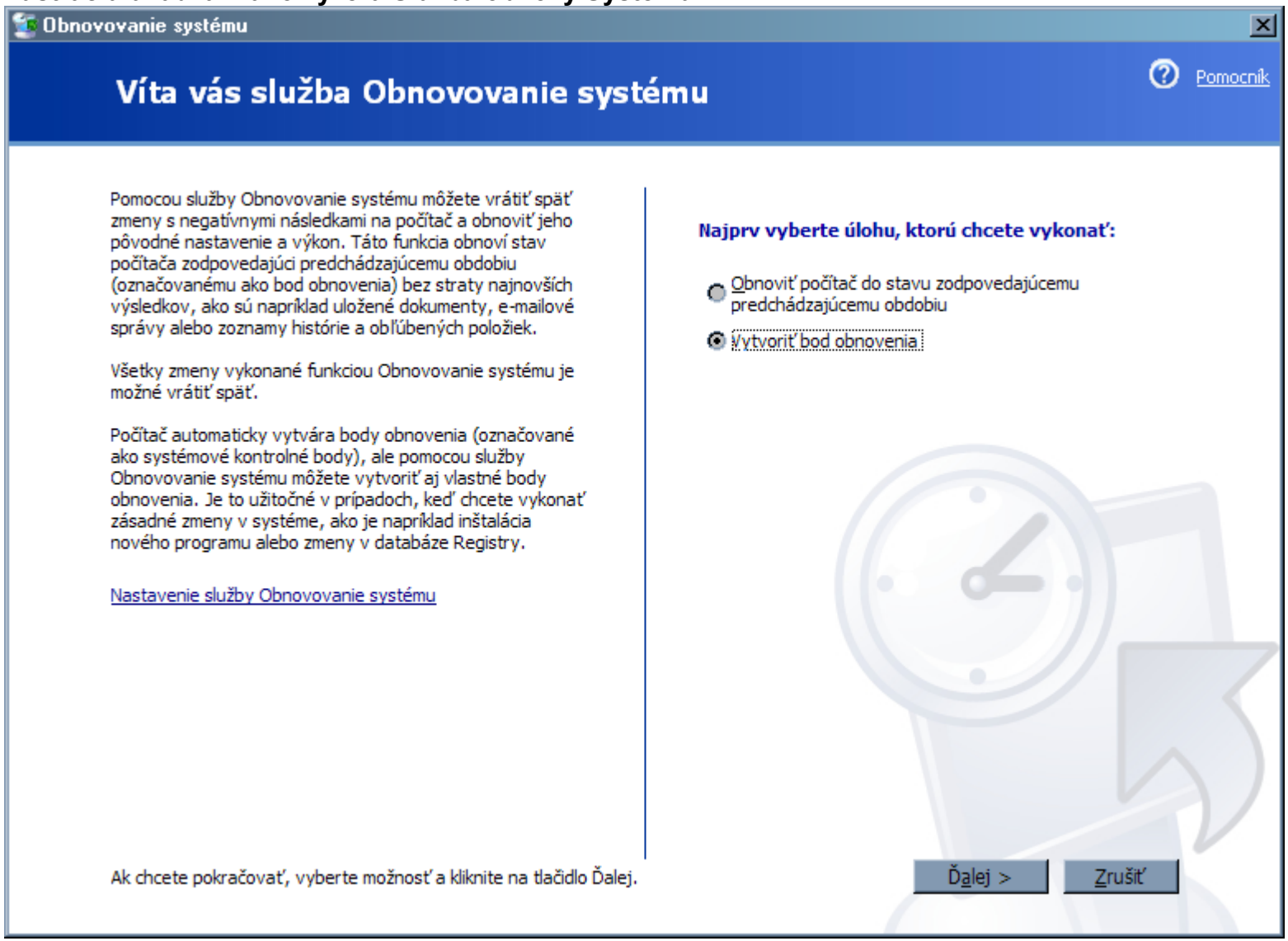
Politika Lokálny Počítač - Konfigurácia Počítača - šablóny pre správu - Windows Components - Windows Update

automatic updates detection frequency
politika určuje čas v hodinách, po uplynutí ktorej / ktorých sa má systém pokúsiť vyhľadať automatické aktualizácie. Tu by som sa pozastavil a poopravil niektoré podľa mňa milné názory, že vraj aktualizácie často spôsobujú problémy. Áno v prípade, že je niekde nejaký problém, či už s ovládačom, nekorektne nainštalovaným

OS, napadnutím počítača nejakým vírusom či trojanom alebo podobnou háveďou, v neposledom rade nainštalovaný OS z pirátskej kópie inštalačného CD (kde nie je žiadna záruka, že nebude niečo pridané / pozmenené). Za celú svoju dlhú mnohoročnú počítačovú prax som sa stretol iba s ojedinelými prípadmi, kedy aktualizácie od MS naozaj spôsobovali nejaký problém. Takže riešenie je jednoduché, nastaviť aktualizácie nie do úplného automatu, ale iba s potvrdením inštalácie už stiahnutých aktualizácií:



kedy je možné sledovať a inštalovať jednotlivé aktualizácie a mať tak o nich aj dostatočný prehľad. Samozrejme, nezabudnúť pravidelne robiť zálohy Službou Obnovovaním Systému (*%SystemRoot%\ServicePackFiles\i386\rstrui.exe*). Pre ilustráciu uvádzam ako vyzerá Služba obnovy Systému:



Politika Lokálny Počítač - Konfigurácia Počítača - šablóny pre správu - System

Turns off the Autoplay
politika určuje, či bude potlačené automatické prehľadávanie / prehrávanie obsahu vymeniteľných médií, ako disketová mechanika, jednotka cd/dvd, USB kľúč, sieťový disk, pozor ale, nastavenie politiky neplatí výhradne iba prehrávanie hudobného obsahu AudioCD ! toto sa dá ale nastaviť v politike:
Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - System
Turns off the Autoplay
ku ktorej sa ale dostaneme neskôr, ešte treba poznamenať, že táto politika je nadriadená politike vyššie spomenutej, konkrétne:
Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - System
Turns off the Autoplay

Dostávame sa k druhej hlavnej vetve politík nástroja "gpedit.msc".

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Windows Components - Internet Explorer

táto politika je samostatnou podmnožinou politík a značne komplexnou, preto sa jej z nedostatku času a priestoru momentálne nemienim venovať. Snáď niekedy v budúcnosti sa k tomu vrátim, aspoň to mám v pláne

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Windows Components - Application Compatibility

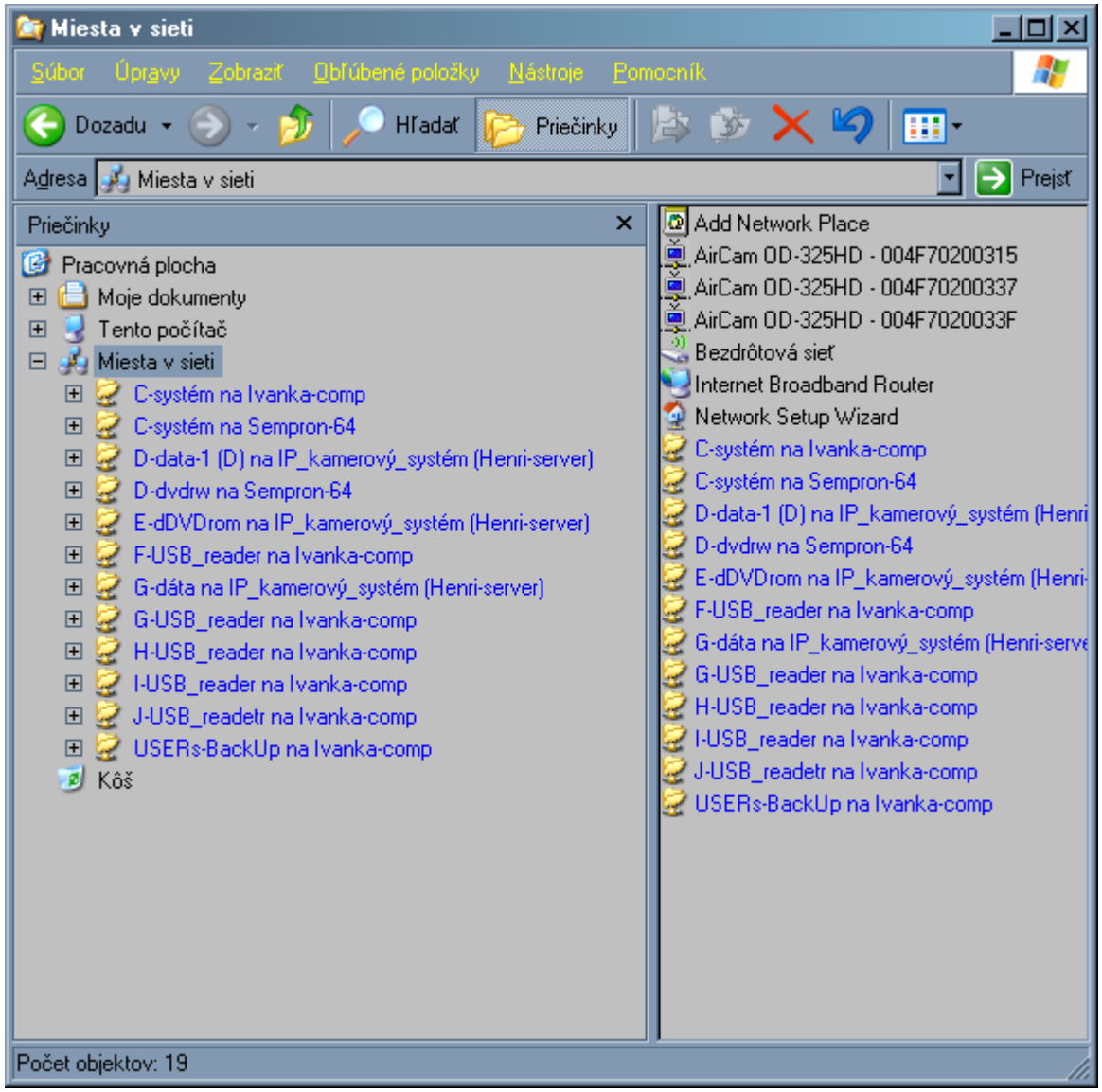
prevent acces to 16-bit applications
politika zabezpečí zamedzeniu prístupu / spúšťaniu k 16 bitovým aplikáciám, prakticky vzaté, zvýši sa o niečo stabilita systému (nie je zaručená kompatibilita a stopercentná funkčnosť 16 bitových aplikácií bežiacich pod 32 bitovým systémom, už zo samotného princípu fungovania) a ušetrí sa aj na systémových prostriedkoch

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Windows Components - Windows Explorer

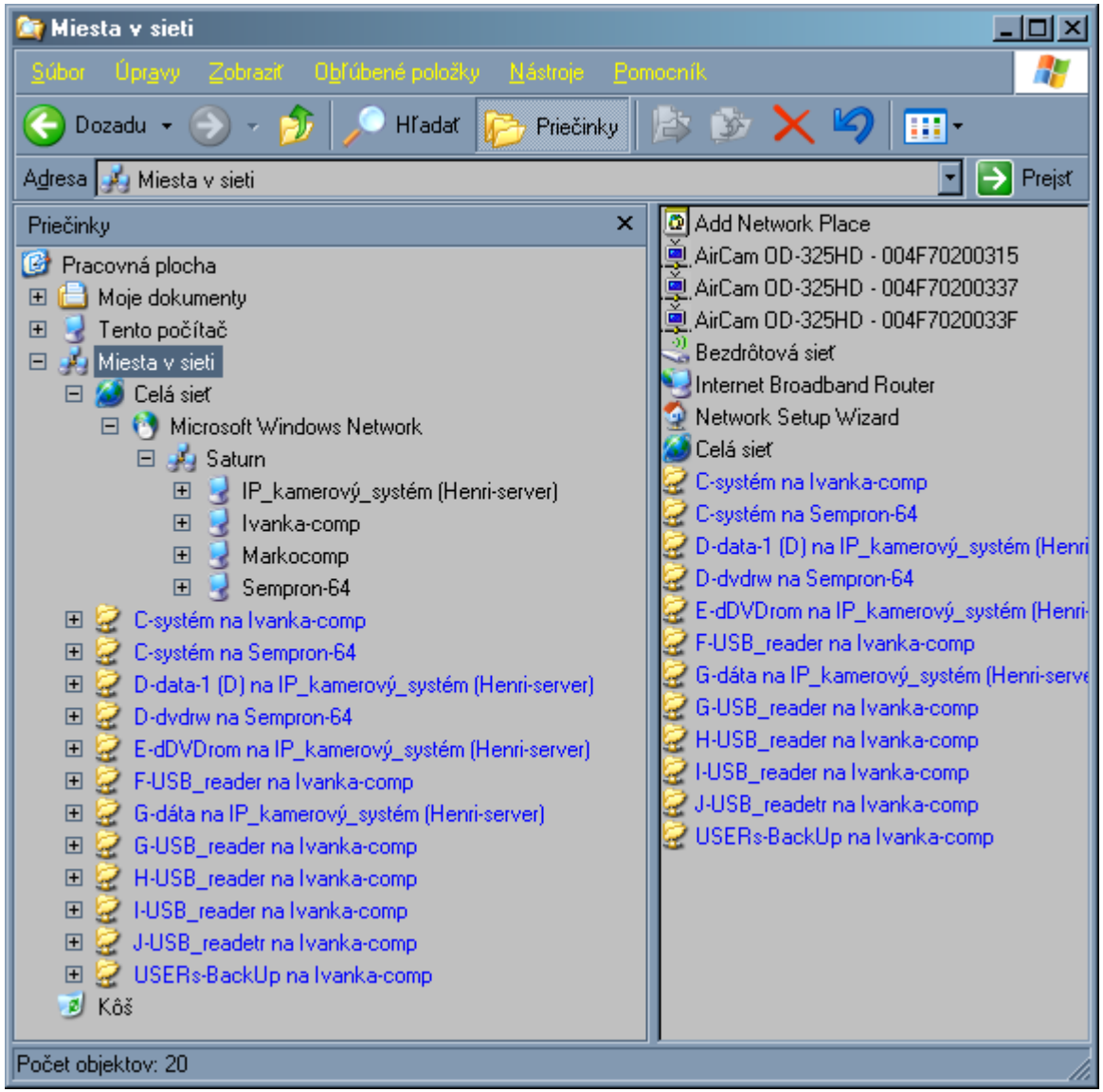
prevent acces to drives from My computer

politika zakáže prístup na jednotlivé mechaniky v závislosti na úrovni nastavenia - tri zákl. úrovne, 1.nenastavené (nič sa nemení vo vzťahu politiky voči nastaveniam), 2. povolené (s možnosťami kombinácií zákazov na jednotlivé mechaniky prípadne skupiny mechaník) a 3. zakázané (teda je implicitne povolený prístup na všetky jednotky systému).
V položke "2. povolené" je možné si vybrať z následovných kombinácií:
Restrict A and B drives only - čiže prakticky to znamená zablokovanie prístupu k FDD jednotkám, ak nie je inou politikou, alebo iným nastavením (napríkald namapovanie sieť. disku na jednotku B určené inak
Restrict D drive only - zablokovanie prístupu k D jednotke (u počítačov s jedným HDD a jednou CD/DVD to teda bude spravidla práve mechanika CD/DVD), nezabúdajme ale, že cez Správcu Diskov sa dá lubovoľnej mechanike okrem systémovej, zmeniť písmeno
Restrict A, B and C drives only - znamená zablokovanie prístupu k FDD jednotkám a k systémovému disku (iba z pohľadu užívateľa, nie systému ako takému)
Restrict A, B,C and d drives only - znamená zablokovanie prístupu k FDD jednotkám, k systémovému disku a k prvému disku za systémovým, či to už bude jednotka CD/DVD alebo ďalší pevný disk počítača
Restrict all drives - znamená zablokovanie prístupu k všetkým jednotkám v systéme
Do not restrict drives - prakticky význam, ako v bode 3. tejto konkrétnej politiky.
Mne osobne trošku chýba možnosť kombinácií, resp. doplnenia lubovolných písmen reprezentujúcich rôzne jednotky, nikde nie je napísané, že počítač musí mať jeden či dva disky s jednou alebo dvomi jednotkami CD/DVD.

No "Entire Networks" in My Network places
politika zakáže zobrazenie okolitých sietí, resp. ich členských počítačov, viď obrázok:

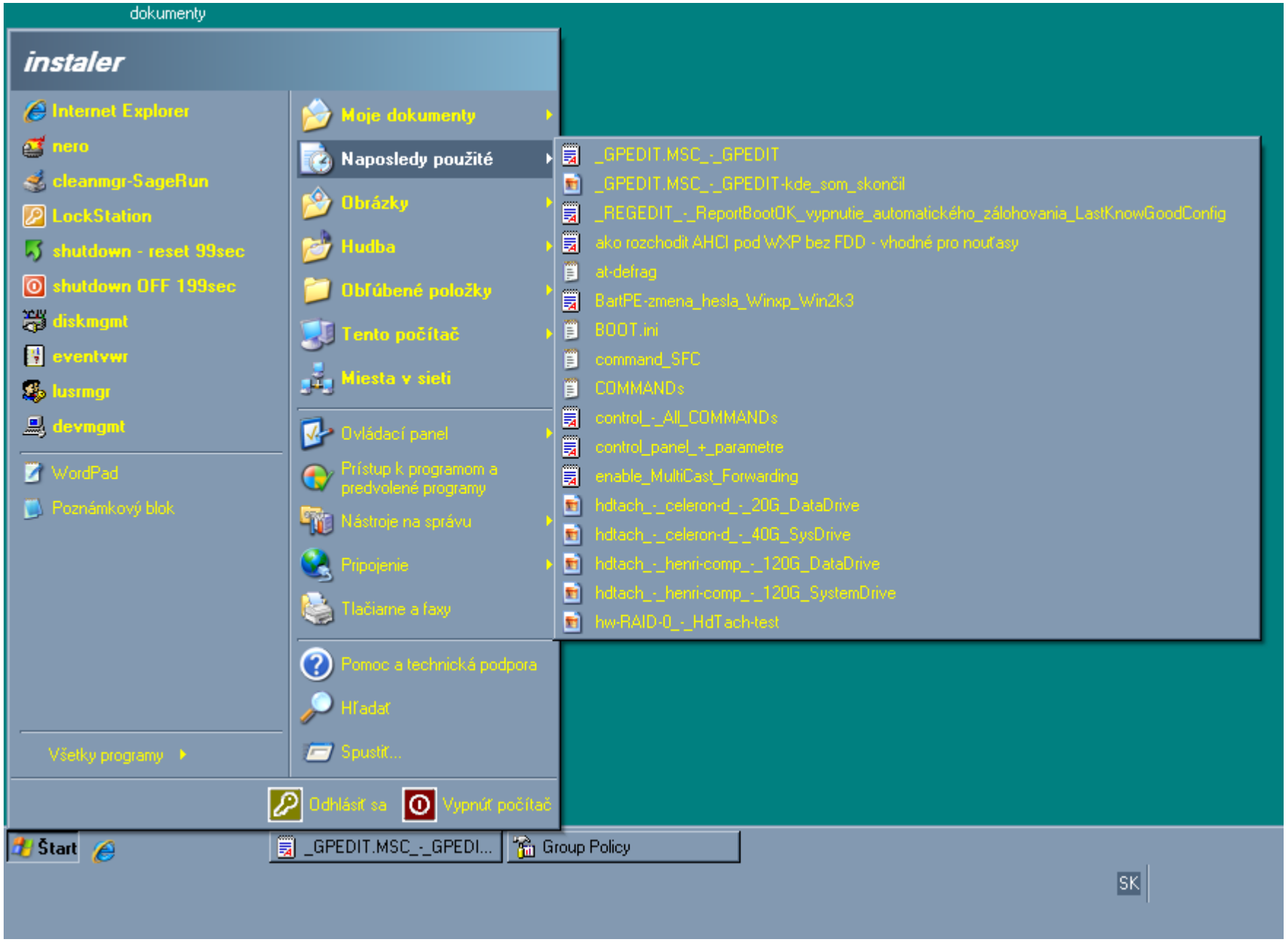


oproti opačnému nastaveniu, teda bez reštrikcie:


Miesta v sieti
Súbor Úpravy Zobraziť Obľúbené položky Nástroje Pomocník
Dozadu
Hľadať
Priečinky
Adresa
Miesta v sieti
Prejsť
Priečinky
Pracovná plocha
Moje dokumenty
Tento počítač
Miesta v sieti
Celá sieť
Microsoft Windows Network
Saturn
IP_kamerový_systém (Henri-server)
Ivanka-comp
Markocomp
Sempron-64
C-systém na Ivanka-comp
C-systém na Sempron-64
D-data-1 (D) na IP_kamerový_systém (Henri-server)
D-dvdrw na Sempron-64
E-dDVDrom na IP_kamerový_systém (Henri-server)
F-USB_reader na Ivanka-comp
G-dáta na IP_kamerový_systém (Henri-server)
G-USB_reader na Ivanka-comp
H-USB_reader na Ivanka-comp
I-USB_reader na Ivanka-comp
J-USB_readetr na Ivanka-comp
USERs-BackUp na Ivanka-comp
Kôš
Add Network Place
AirCam OD-325HD - 004F70200315
AirCam OD-325HD - 004F70200337
AirCam OD-325HD - 004F7020033F
Bezdrôtová sieť
Internet Broadband Router
Network Setup Wizard
Celá sieť
C-systém na Ivanka-comp
C-systém na Sempron-64
D-data-1 (D) na IP_kamerový_systém (Henri
D-dvdrw na Sempron-64
E-dDVDrom na IP_kamerový_systém (Henri-
F-USB_reader na Ivanka-comp
G-dáta na IP_kamerový_systém (Henri-serve
G-USB_reader na Ivanka-comp
H-USB_reader na Ivanka-comp
I-USB_reader na Ivanka-comp
J-USB_readetr na Ivanka-comp
USERs-BackUp na Ivanka-comp
Počet objektov: 20

Maximum number of recent documents

politika určuje počet zobrazovaných dokumentov v Štart Menu v položke posledných použitých dokumentov. S obľubou nastavujem počet aspoň na 40 či 50. Zdá sa mi to stále rýchlejšie, ako otvárať konkrétny príslušný program, potom pri otváraní dokumentu dokument ešte aj následne vyhľadať. Samozrejme existujú aj iné možnosťi a to napríklad urobiť zástupcov na plochu, ale si neviem dosť dobre predstaviť neprehľadnosť plochy na ktorej by malo byť 50 dokumentov.


dokumenty
instaler
Internet Explorer
nero
cleanmgr-SageRun
LockStation
shutdown - reset 99sec
shutdown OFF 199sec
diskmgmt
eventvwr
lusrmgr
devmgmt
WordPad
Poznámkový blok
Všetky programy
Moje dokumenty
Naposledy použité
Obrázky
Hudba
Obľúbené položky
Tento počítač
Miesta v sieti
Ovládací panel
Prístup k programom a predvolené programy
Nástroje na správu
Pripojenie
Tlačiarne a faxy
Pomoc a technická podpora
Hľadať
Spustiť...
Odhlásiť sa
Vypnúť počítač
GPEDIT.MSC-_GPEDIT
GPEDIT.MSC-_GPEDIT-kde_som_skončil
REGEDIT-_ReportBootOK_vypnutie_automatického_zálohovania_LastKnowGoodConfig
ako rozchodit AHCI pod WXP bez FDD - vhodné pro nouťasy
at-defrag
BartPE-zmena_hesla_Winxp_Win2k3
BOOT.ini
command_SFC
COMMANDs
control_-_All_COMMANDs
control_panel_+_parametre
enable_MultiCast_Forwarding
hdtach_-_celeron-d_-_20G_DataDrive
hdtach_-_celeron-d_-_40G_SysDrive
hdtach_-_henri-comp_-_120G_DataDrive
hdtach_-_henri-comp_-_120G_SystemDrive
hw-RAID-0_-_HdTach-test
Štart
GPEDIT.MSC-_GPEDI...
Group Policy
SK

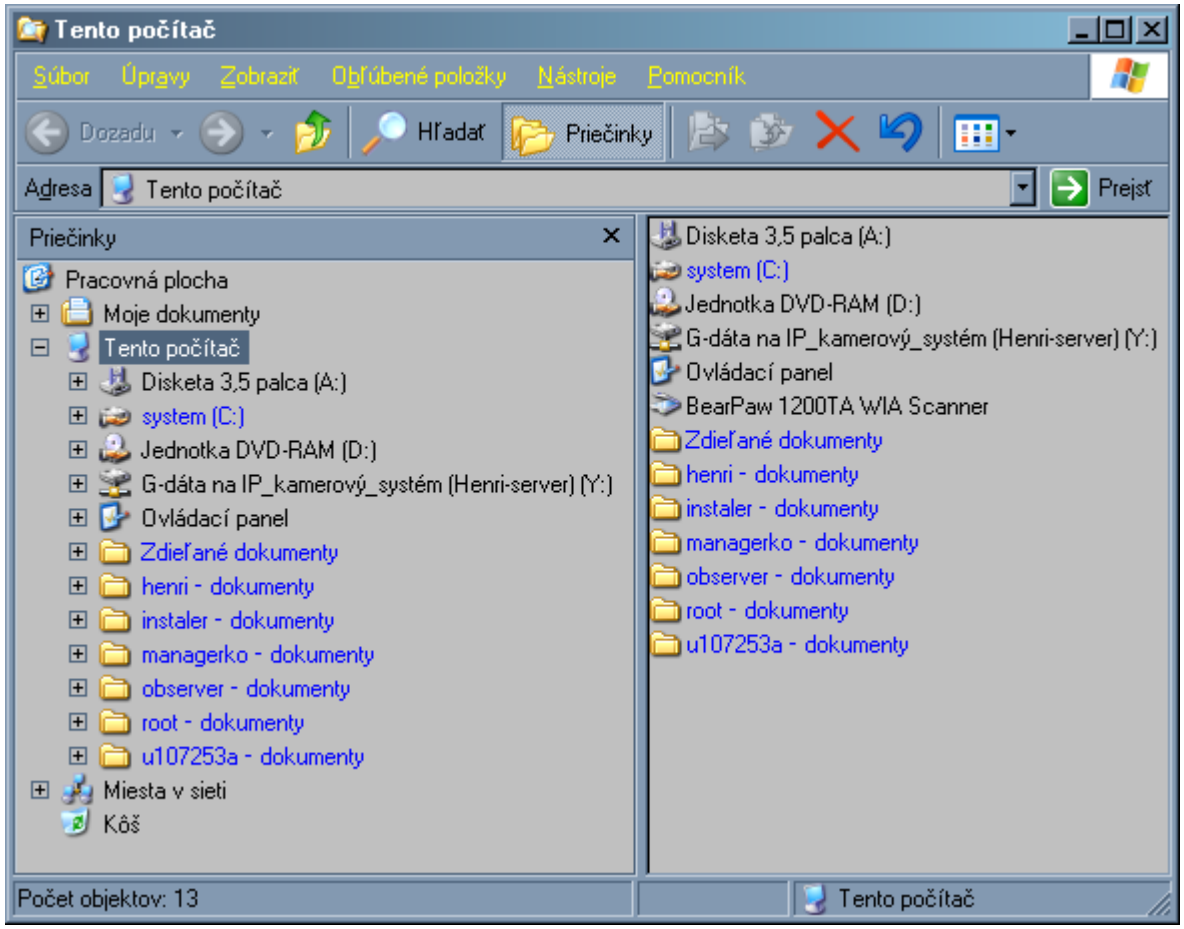
Remove CD Burning features
politika zakáže vo Windows Explorer-i prístup k zápisu na médiá CD/DVD RW/RAM

Do not move deleted files to Recycle Bin
politika zakáže mazanie súborov / adresárov cez kôš, teda súbor / adresár je prakticky nenávratne vymazaný (za predpokladu, že sa nemení súborová štruktúra, je do značnej miery možné aj takto vymazané dáta zreštaurovať špecializovaným programom, na to určeným, ale úspech nie je zaručený na 100 percent a kvalitné programy k tomu určené sú drahé, resp. služby špecializovaných firiem sa tomu venujúcich)

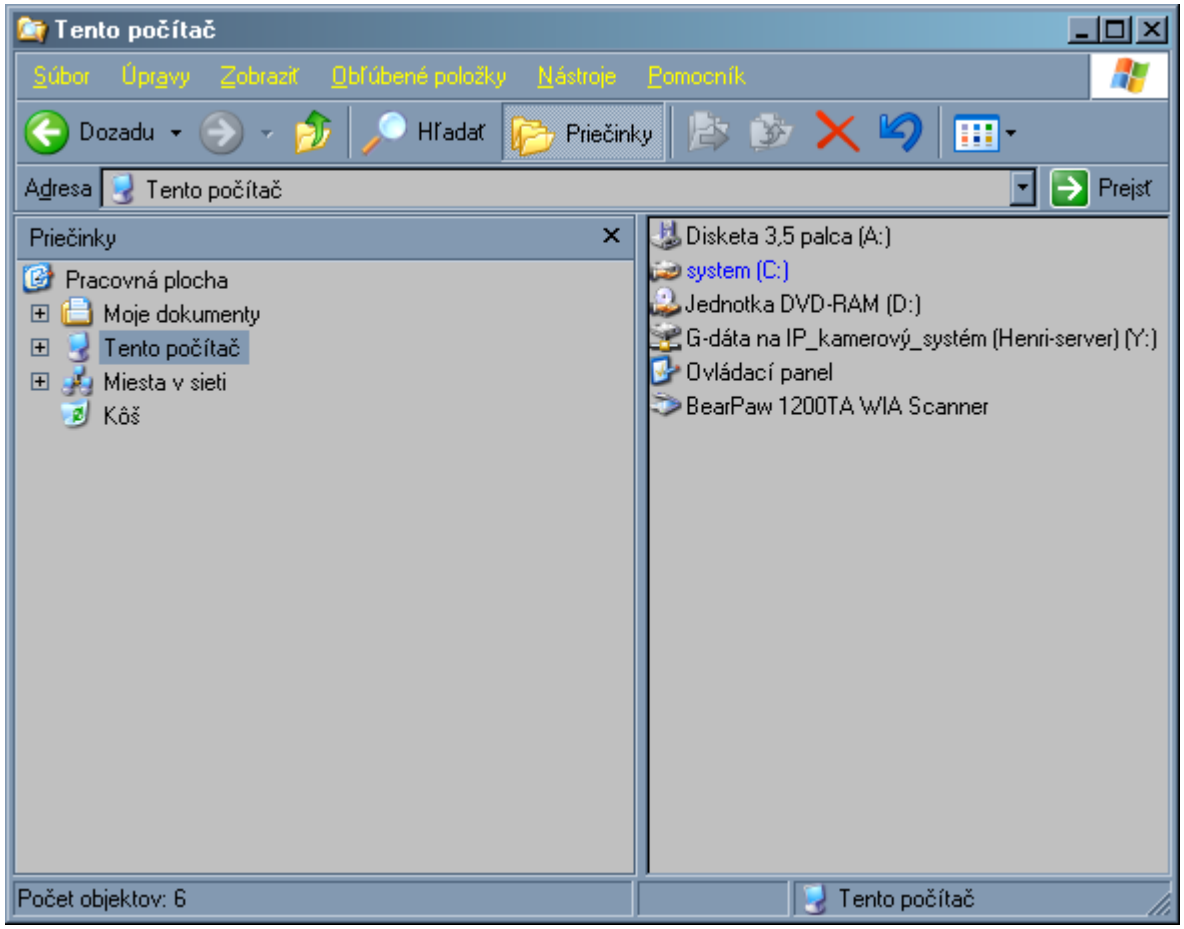
Display confirmation dialog when deleting files
politika určuje, že pri mazaní súborov / adresárov sa systém vždy opýta na potvrdenie vymazania

Maximum allowed Recycle Bin size
politika určuje, aké má byť percentuálne obsadenie maximálneho miesta na disku / diskoch pre Kôš

Remove Shared Documents from My Computer
politika určuje, či má byť alebo nemá byť zobrazovaný a prístupný adresár so zdieľanými dokumentami, základné nastavenie, teda "nenastavené" vyzerá takto:



a po aplikovaní politiky:



Turn off caching of thumbnails pictures

politika určuje, či má byť deaktivované predčítanie (kešovanie) obrázkov vo Windows Exploreri pri pohľade "Zobraziť-Miniatúry", na slabších počítačoch (so slabším procesorom a s malou pamäťou RAM) odporúčam toto nastavenie aktivovať, na výkonnejších naopak deaktivovať, bude sa načítavať obsah náhľadov s obrázkami rozhodne rýchlejšie

Turn off Windows+X hotkeys

politika určuje, či má byť deaktivované použitie známych klávesových skratiek (Win+L, Win+E, Win+R a pod.)

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Windows Components - Windows Messenger

Do not allow Windows Messenger to be run
politika určuje, či má byť deaktivované automatické spúšťanie WindowsMessenger (známy OnLine komunitáror {niečo ako slabší odvar Skype}), je možné to nastaviť aj cez Politika Lokálny Počítač - Konfigurácia Počítača - šablóny pre správu - Windows Components - Windows Messenger, ale nastavenie cez Konfig Počítača má prednosť pred nastavením cez Konfig. Používateľa

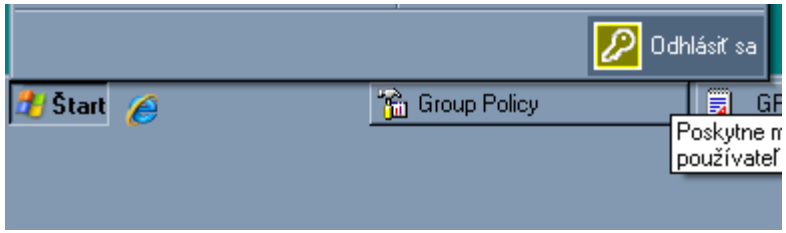
Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - start menu and Taskbar

Remove Run menu from Start Menu
politika zabezpečí odobratie položky "spustiť" zo Štart Menu

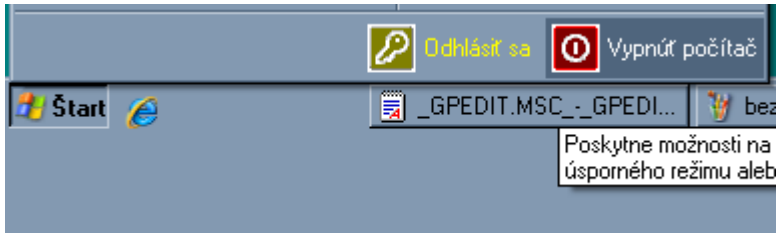
Add LogOff to the Start Menu
politika zabezpečí pridanie položky "odhlásenie" do Štart Menu

Remove LogOff from the Start Menu
politika zabezpečí odstránenie položky "odhlásenie" do Štart Menu

Remove and prevent acces to the ShutDown command
politika zabezpečí odstránenie položky Vypnutie Počítača zo Štart Menu:



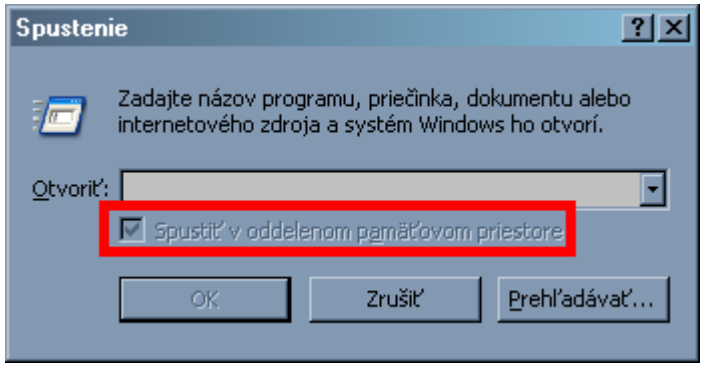
na rozdiel od neaplikovanej politiky:



Do not keep history of recently opened documents
politika zabezpečí, že sa nezachová zoznam naposledy použitých dokumentov

Clear history of recently opened documents
politika zabezpečí, že sa počas odhlasovania / reštartu vymaže zoznam naposledy použitých dokumentov

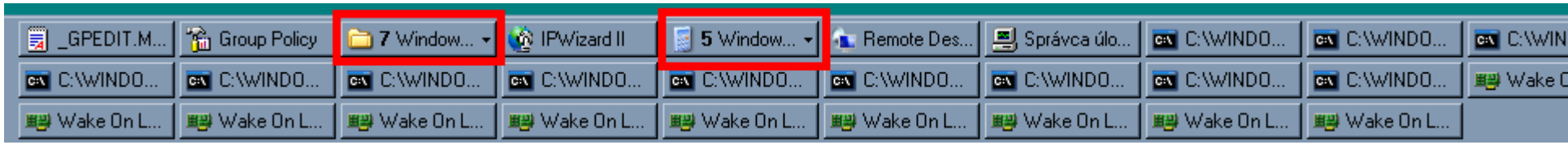
Add "Run in Separate Memory Space" check box to Run dialog box
politika zabezpečí, že sa v štart menu (štart, spustiť)zobrazí možnosť odfajknutia spustenia programu / aplikácie / dokumentu v oddelenom pamäťovom priestore



gray unavailable Windows Installer programs Start Menu shortcuts
politika zabezpečí, že sa v Štart Menu bude rozdielne zobrazovať program plne nainštalovaný a nainštalovaný iba čiastočne (napr. menu programu bude vyšedené {aspoň to tvrdí MS}) a vyšedené môžu byť tiež položky momentálne neprístupné, zakázané, či neaktivované alebo inak nefunkčné

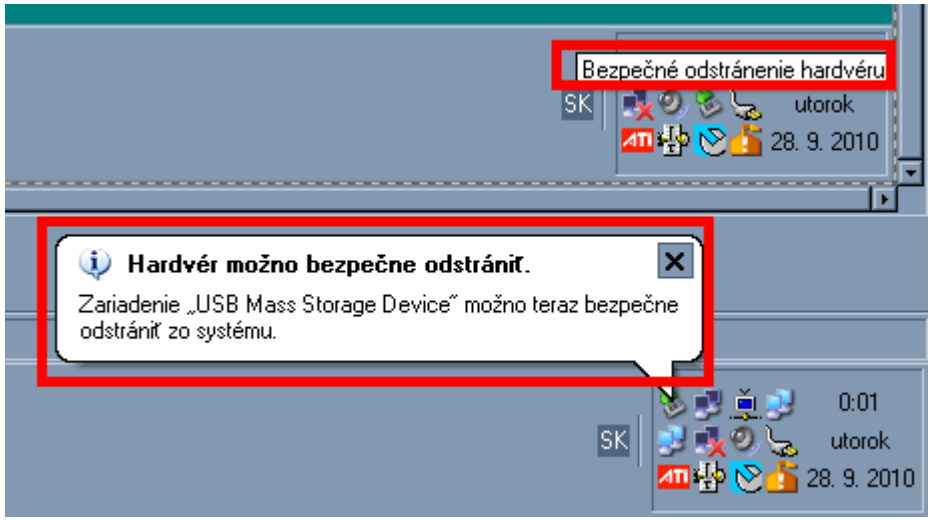
Prevent grouping of taskbar items

politika zabezpečí, že po naplnení panela úloh sa nebudú rovnaké programy spájať do skupín, alebo opačným nastavením budú:



Remove Balloon Tips on Start Menu items

politika zabezpečí odstránenie balónových-bublinkových typov zo Štart Menu a z Panela Úloh, alebo naopak:



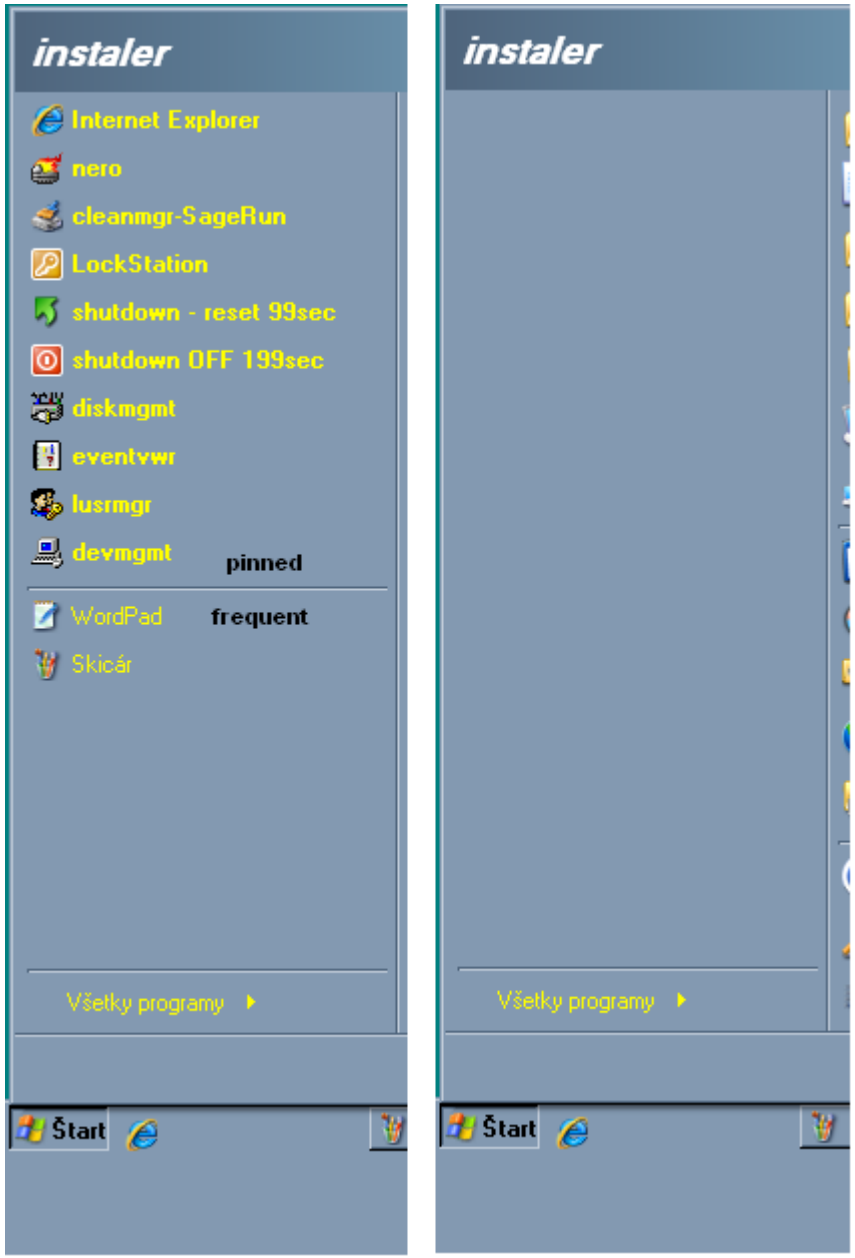
Remove pinned programs list from the Start Menu

politika zabezpečí odstránenie "prišpendlených" programov zo Štart Menu

Remove frequented programs list from the Start Menu

politika zabezpečí odstránenie "častých" programov zo Štart Menu

viď spoločný obrázok:


instaler
Internet Explorer
nero
cleanmgr-SageRun
LockStation
shutdown - reset 99sec
shutdown OFF 199sec
diskmgmt
eventvwr
lusrmgr
devmgmt
pinned
WordPad
frequent
Skicár
Všetky programy
Štart
instaler
Všetky programy
Štart

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Desktop - Active Desktop

Enable Active Desktop
politika povoľuje alebo zakazuje zobrazenie plochy ako WEB stránky
nasledujúci obrázok zobrazuje stav povolenej WEB stránky na ploche:

W Obrázky py Prekladač Blogy Aktualizácie Gmail viac ▼

Moje dokumenty

Odkaz na _GPEDIT....

Tento počítač

Zdieľané dokumenty

Obrázky

Miesta v sieti

Windows Media Player

na webe

Stránky v slovenčine

Stránky z (zo) Slovenska

Kôš

Kedykoľvek

Po posledných dňoch: 2

Internet Explorer

zobrazenie

Webové stránky s obrázkami

IP Wizard II

pástrojov

Odkaz na _GPEDIT.M...

Mozilla Firefox

server

Hľadať

Približný počet výsledkov: 438 000 000 (0,16 sekúnd)

Rozšírené vyhľadávanie

Server - Wikipédia

Server (z angl. to serve - slúžiť, poskytovať službu) softvér, ktorý v rámci počítačovej siete zastáva v hierarchii nadradené miesto vzhľadom na ...

sk.wikipedia.org/wiki/**Server** - V pamäti - Podobné

Server.sk

www.**Server**.sk - kompletný katalóg internetu, vyhľadávanie, nové články, správy, agentúrne správy, domov, zahraničie, šport, kultúra.

JobServer - RealityServer - FitServer - BackStage

www.**server**.sk/ - V pamäti - Podobné

PC.**SERVER**.SK

27. sep. 2010 ...

software,hardware,internet,bezpečnosť,security,programovanie,ASP,ASP.NET,VB,C#,FLASH,DELPHI,.NET,PHP,T-SQL,SQL,JAVA,script,multimedia,hry ...

pc.**server**.sk/ - V pamäti - Podobné

Obrázky pre dopyt **server** - Nahlásenie obrázkov

Server | Ubuntu - [Preložiť túto stránku]

Lean, fast and powerful, Ubuntu **Server** delivers services reliably, predictably and economically – and it easily integrates with your existing infrastructure ...

www.ubuntu.com/**server** - V pamäti

VMware **Server**, Free Virtualization Download for Virtual **Server** ... - [Preložiť túto stránku]

Start your virtual **server** consolidation with VMware **Server**, a free VMware download. Reduce IT costs and improve flexibility, improve business continuity, ...

www.vmware.com › Products › Datacenter Products - V pamäti - Podobné

Sponzorované

Dedikovan

Sklad HW, p

Neobmezený

www.datacar

Server.

Uchýľte sa k

Digitálna ma

WebSupport.

Server?

Server hosti

Bezpečný **se**

www.yegon.s

Servery

Dedikované s

Garancia výk

www.domeny

Servery lac

Výkonné ser

domáce použ

Alza.sk/**Serv**

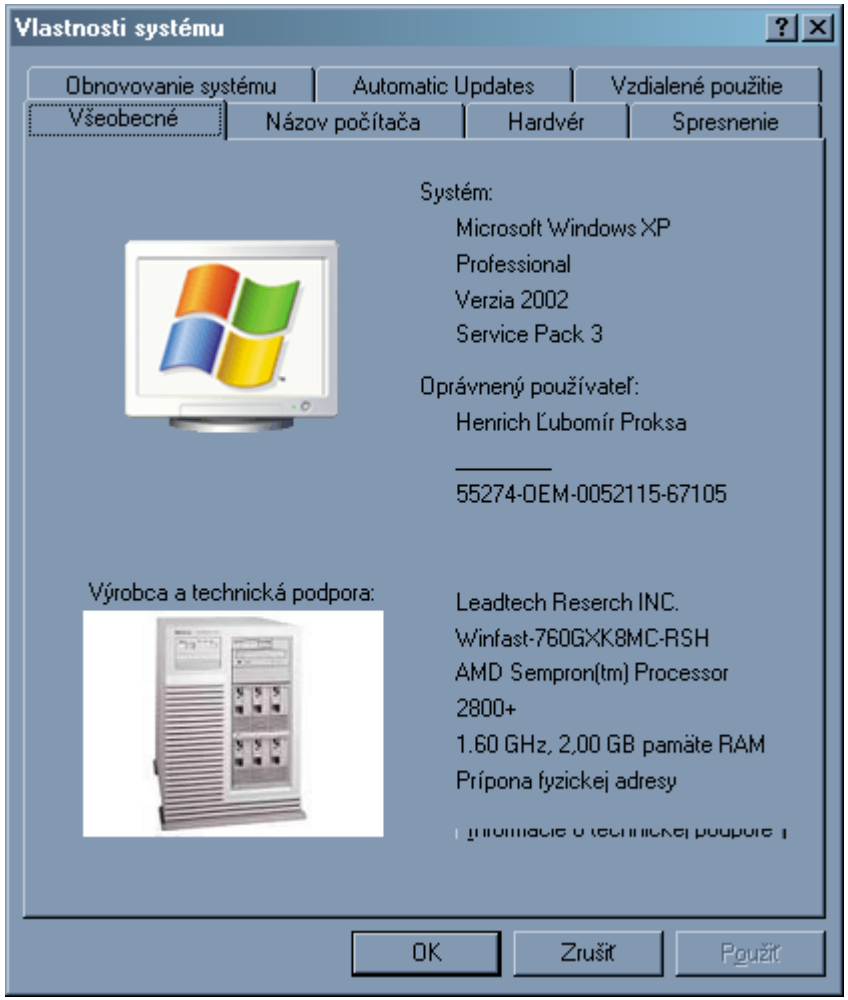
Tu môže byť zo

Štart

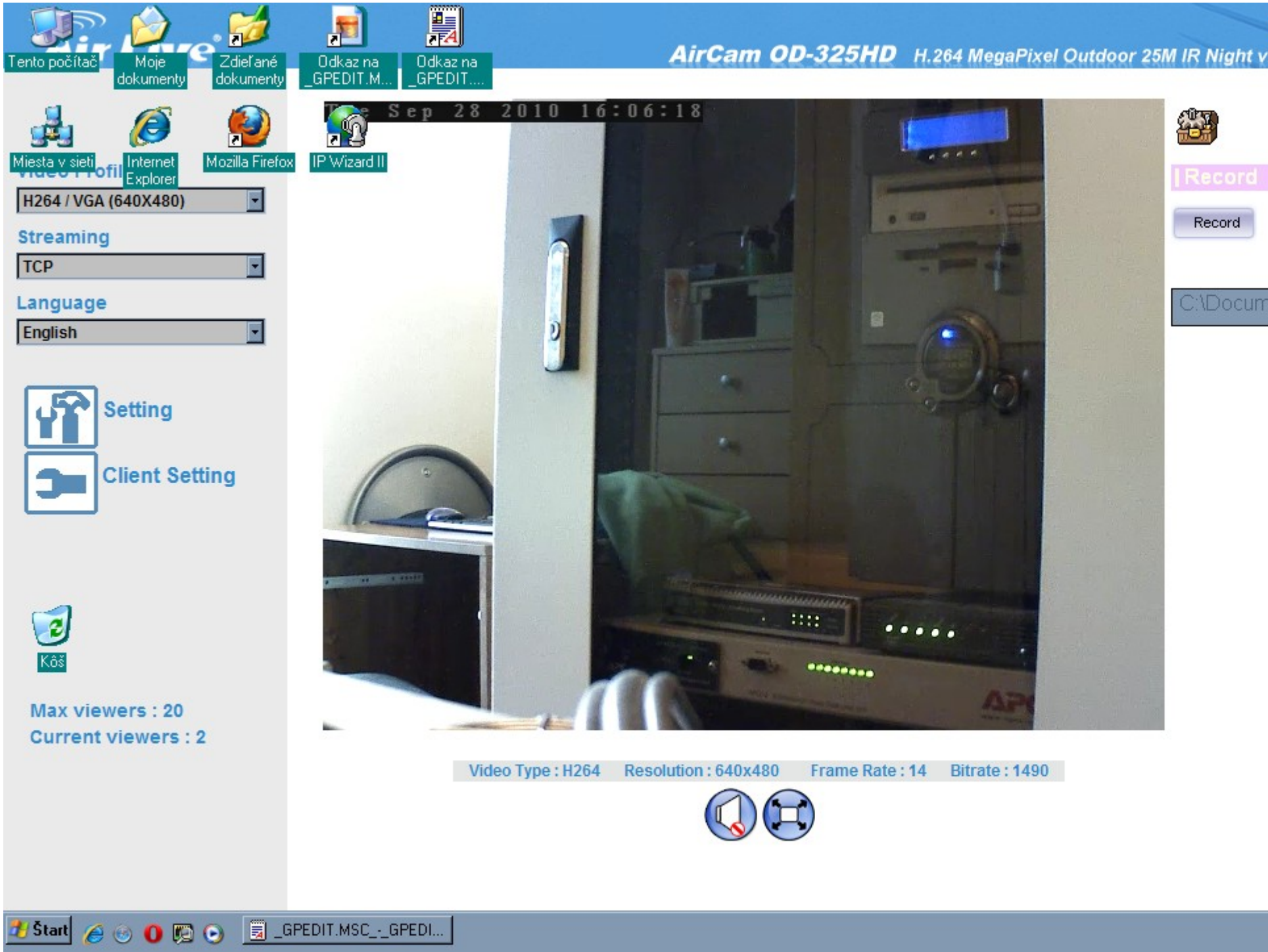
Group Policy

GPEDIT.MSC-_GPEDI...

treba povedať, že toto nastavenie spomaľuje systém (taktiež sa pripravte na úbytok pamäte RAM zhruba v rozsahu od 20MB - 150MB, je to len naozaj veľmi hrubý údaj, ktorý je ovplivnený rôznimi inými faktormi, ako napríklad počet ovládačov v RAM, počet prihlásených užívateľov, množstvo pospúšťaných programov, aplikácií a služieb, vyladenie operačného systému, HW konfigurácia počítača a pod.), síce citeľnú stratu výkonu som na tomto testovacom počítači nepostrehol, ale mierny pokles predsa len hej:



teda je na Vás, či radšej zakázať a predísť tak problémom s Pracovnou plochou, minimálne s rozhádzaním ikôn, na čo sú niektorý užívatelia mimoriadne háklivý { tiež patrím medz nich :-) } alebo na druhej strane, ak je dostatočne výkonný počítač a používate napríklad sledovanie cez IP kameru, v takomto prípade toto riešenie odoprúčam, viď nasledujúci obrázok:

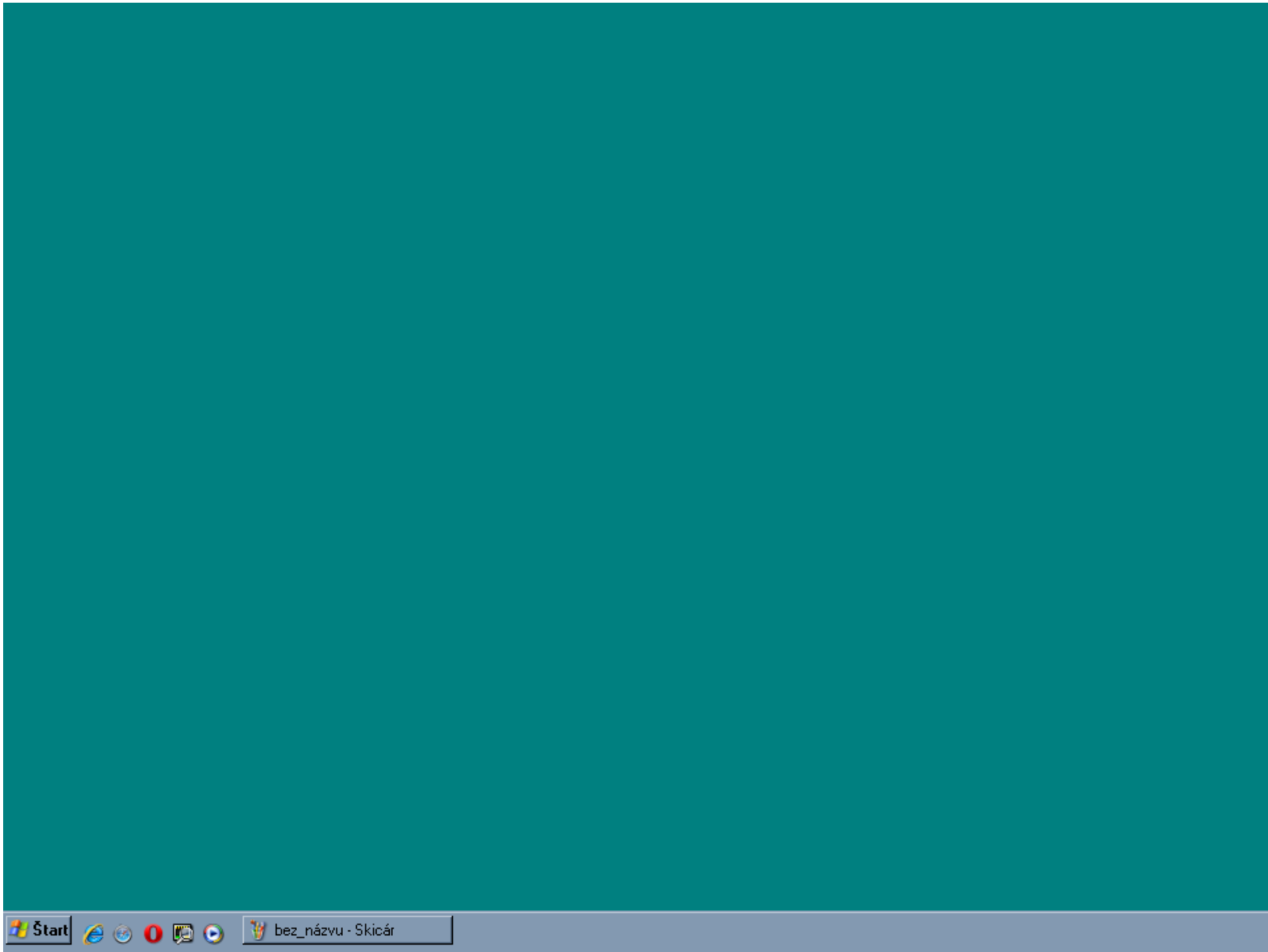

Tento počítač
Moje dokumenty
Zdieľané dokumenty
Odkaz na _GPEDIT.M...
Odkaz na _GPEDIT....
AirCam OD-325HD H.264 MegaPixel Outdoor 25M IR Night v
Miesta v sieti
Internet Explorer
Mozilla Firefox
IP Wizard II
Video Profile
H264 / VGA (640X480)
Streaming
TCP
Language
English
Setting
Client Setting
Kôš
Max viewers : 20
Current viewers : 2
Sep 28 2010 16:06:18
Record
Record
C:\Docum
Video Type : H264
Resolution : 640x480
Frame Rate : 14
Bitrate : 1490
Štart
GPEDIT.MSC-_GPEDI...

Disable Active Desktop
politika zakazuje alebo povoľuje zobrazenie plochy ako WEB stránky. Prakticky, opak politiky spomenutej vyššie. Ak je táto politika povolená spolu s politikou predchdádzajúcou, táto bude ignorovaná predchádzajúcou. Spolu obidve politiky budú ignorované, ak bude aplikovaná politika (povolená):
Politika Lokálny Počítač - Konfigurácia Počítača - šablóny pre správu - Windows Components - Windows Explorer / Turn off shell protocol protected mode
touto posledne spomenutou politikou teda zabezpečíme, že žiadny užívateľ si nebude môcť meniť nastavenie plochy, čo sa týma zobrazovania ako WEB stránky (aspoň to tvrdí MS, mne sa ale aplikáciou tejto politiky {Politika Lokálny Počítač - Konfigurácia Počítača - šablóny pre správu - Windows Components - Windows Explorer / Turn off shell protocol protected mode} nepodarilo dosiahnuť vypnutie aktívnej WEB plochy)

Disable all items
aplikáciou tejto politiky potvrdíme zákaz aktívnej WEB plochy a je jedno, čo je nastavené v dvoch predošlých politikách

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Desktop

Hide and disable all items on the desktop
aktivovaním tejto politiky zabezpečíme úplny zákaz všetkých položiek Plochy (teda aj ikôn a zástupcov), vrátene aktívneho WEB obsahu, ako vidieť na nasledujúcom obrázku:


Štart
bez_názvu - Skicár

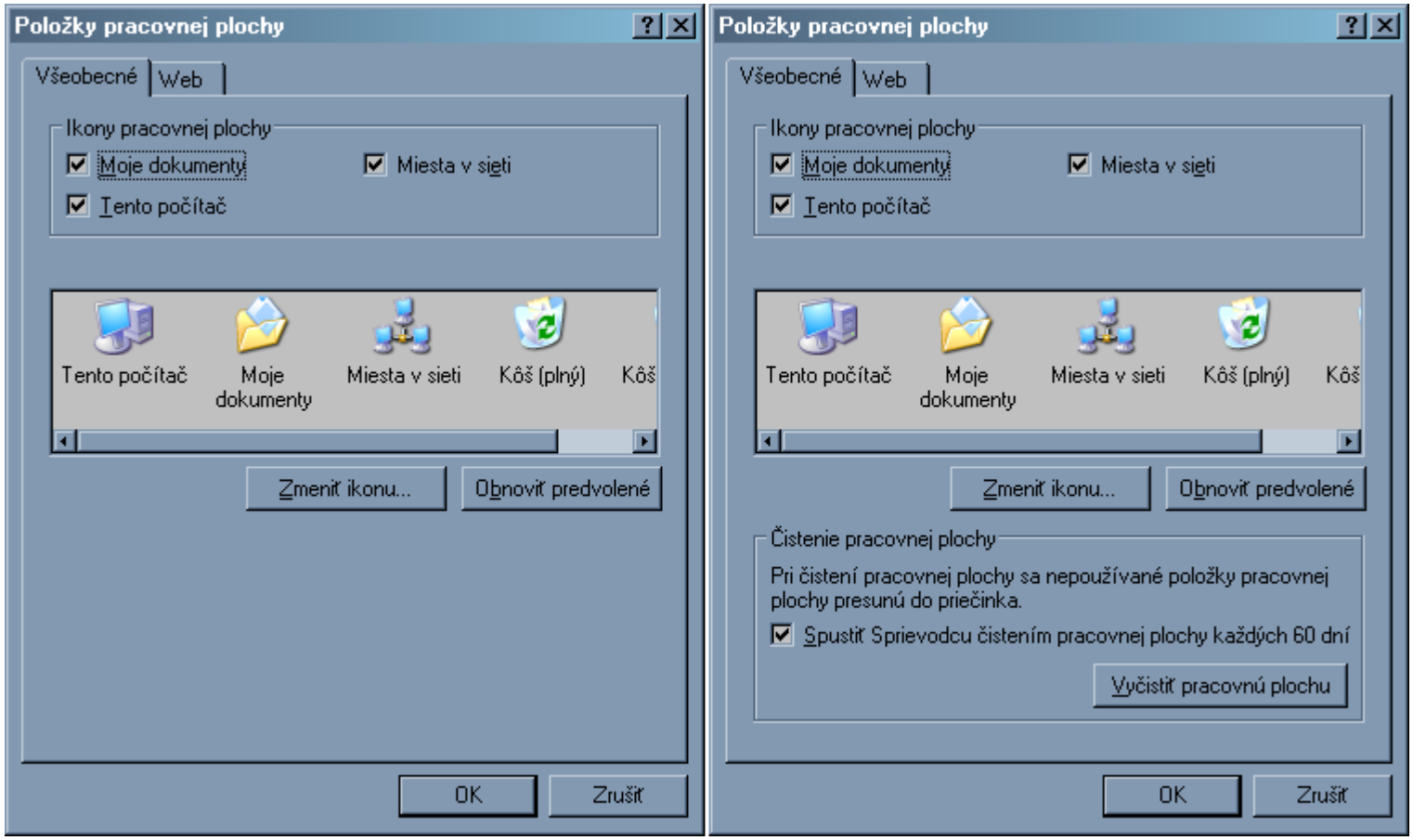
zákaz platí na nastavenie priamo z Plochy (zmiznú úplne všetky ikony), tiež je platný na nastavenie cez ŠtartMenu.

Hide Internet Explorer icon the desktop
aktivovaním tejto politiky zabezpečíme zákaz zobrazenia ikony Internet Explorera na ploche.

Prohibit user changing My Documents path
aktivovaním tejto politiky zakážeme, alebo naopak povolíme, ak nie je inou politikou povedané inak, zmenu umiestnenia užívateľských dát (typicky %UserProfile%\My Documents)

Dont save settings at exit
aktivovaním tejto politiky zakážeme uloženie niektorých nových / zmenených položiek plochy (napr. pozície okien, veľkosti okien, veľkosť / poozícia TaskBaru a pod.), pozor, nastavenie sa nedotkne ikôn

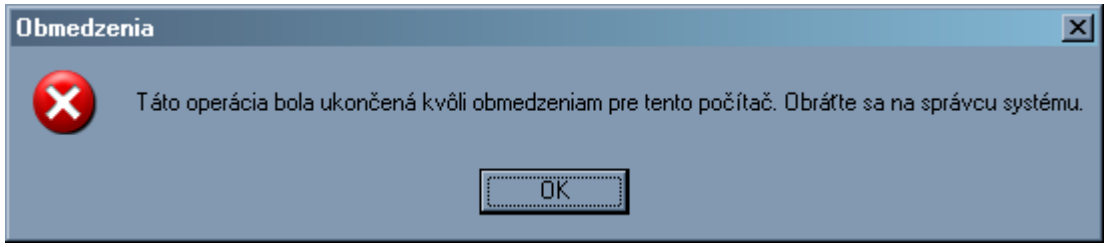
Remove the Desktop Cleanup Wizard
aktivovaním tejto politiky odstránime z Plochy možnosť čistenia Prac. Plochy, viď obr. nižšie:



Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Control Panel

Prohibit acces to the Control Panel

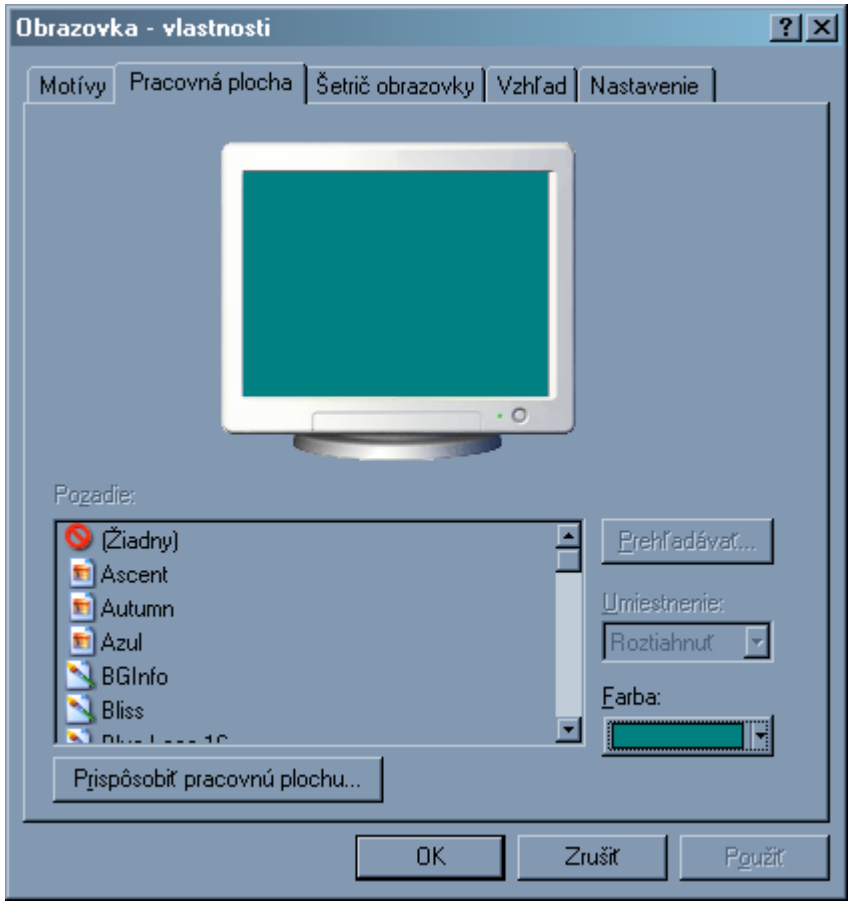
aktivovaním tejto politiky zabezpečíme zákaz zobrazenia Ovládacieho Panelu(Control Panel), z menu sa odstráni až po reštarte systému, a samozrejme aj zákaz jeho použitia (bude platný okamžite po aplikovaní politiky), čiže nebude možné meniť žiadne vlastnosti (klávesnica, myš, obrazovka, tlačiarne a pod.). Pri pokuse o spustenie akejkoľvek položky z menu Ovládacieho Panelu alebo cez príkazový riadok príde hlásenie:



Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - Control Panel - Display

Prevent changing wallpaper

aktivovaním tejto politiky zabezpečíme zákaz / povolenie zobrazenia obrázku na pozadí Pracovnej Plochy, ako aj zmeny obrázku za iný:



Password protect the screen saver

aktivovaním tejto politiky zabezpečíme, že šetrič obrazovky sa pri aktivovaní vždy uzamkne heslom

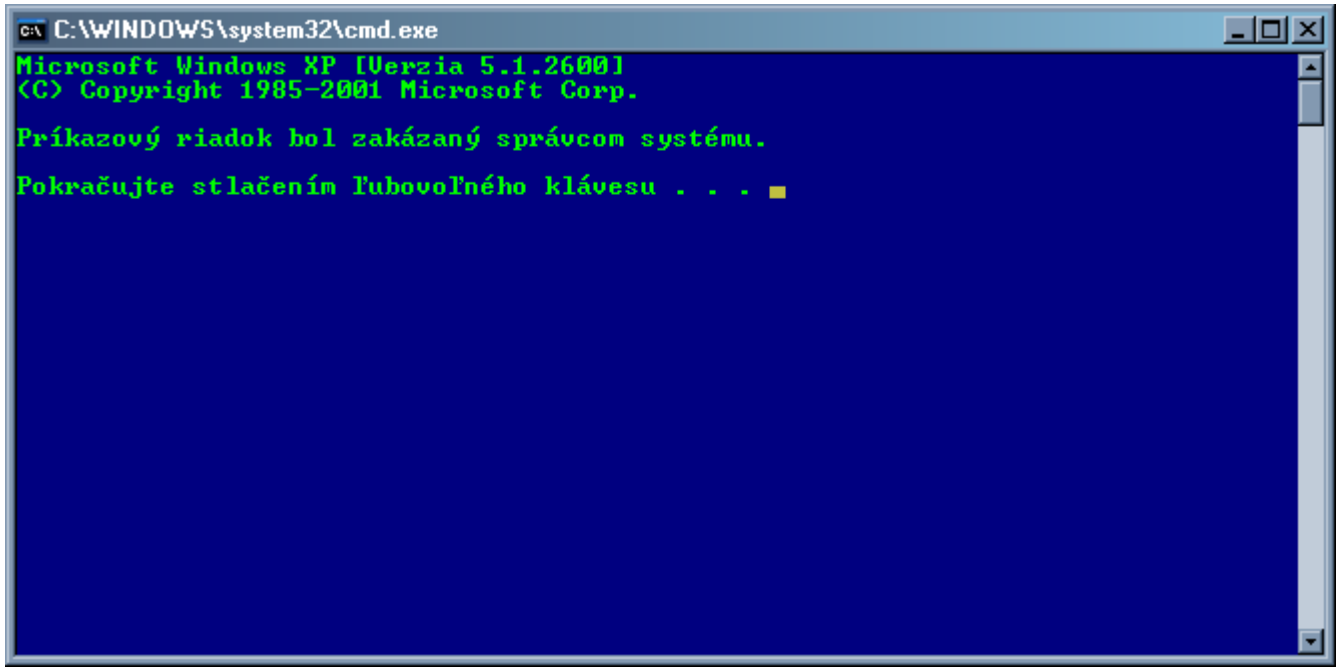
Screen Saver timeout

aktivovaním tejto politiky zabezpečíme pevné nastavenie času spúšťania šetriča (bez ohľadu na to, aký je použitý)

Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - System

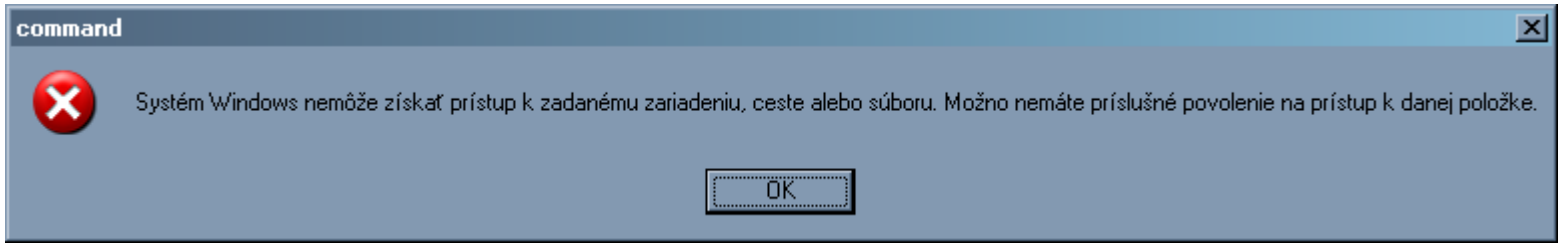
Prevent acces to the command prompt

politika zákaže prístup k príkazovému riadku (cmd):



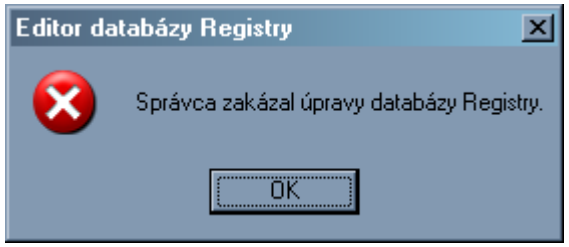
Prevent acces to the command prompt

politika zákaže prístup k príkazovému riadku (command):



Prevent acces registry editing tools

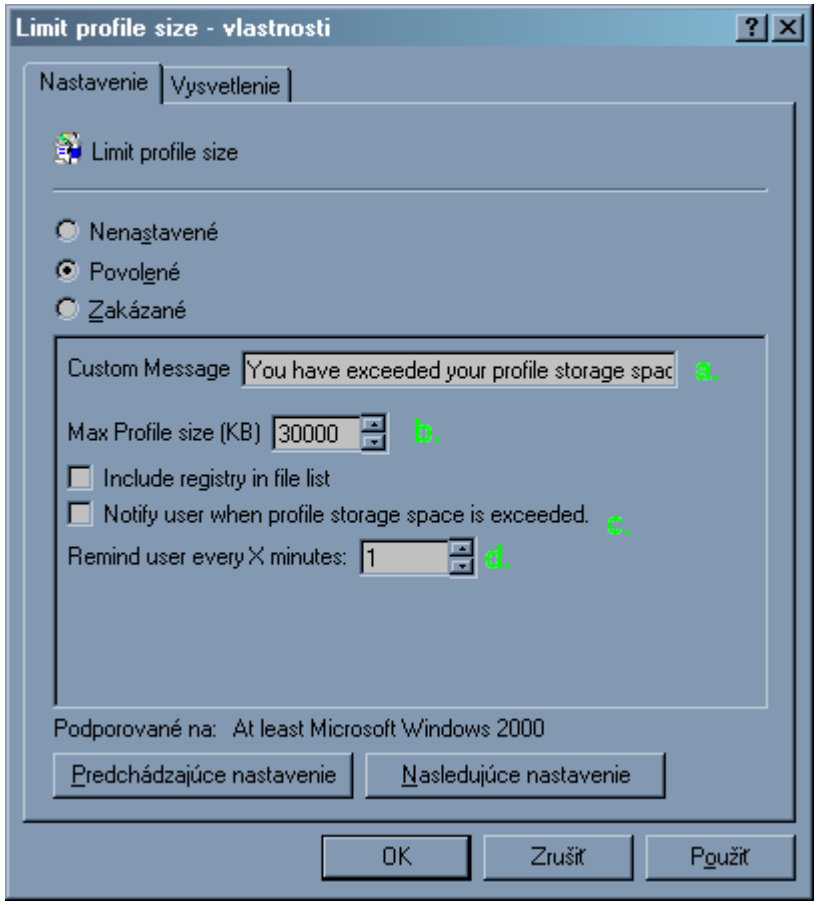
politika zákaže prístup k editoru Registrov:



Turn off Autoplay
politika zákaže automatické prehrávanie / prehliadanie / otváranie buď iba jednotiek CD/DVD (CD-ROM drives) alebo aj ostatných vymeniteľných, teda aj USB kľúčov a aj čerstvo namapovaných sieťových diskov (All drives)

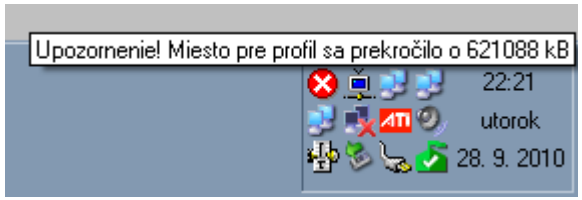
Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - System - User Profiles

Limit profile size
politika obmedzí veľkosť užívateľského profilu určenú v kB:



v bode a. si možme doplniť text informujúci o prekorečení limitu veľkosti profilu užívateľa
v bode b. určujeme maximálnu veľkosť profilu užívateľa, pri ktorej už bude chodiť hláška v intervaloch rádovo v minutách nastavených v bode d.
v bode c. určímne fajkou, že užívateľ bude informovaný v pravidelných časových intervaloch nastavených v bode d. hláškou o prekorečení limitu veľkosti profilu užívateľa:

a v Paneli Úloh sa bude zobrazovať informácia:



Politika Lokálny Počítač - Konfigurácia Používateľa - šablóny pre správu - System - Power Management

Prompt for password on resume from hybernate / suspend
politika prikáže pri "zobudení" počítača zo spánku alebo "prebratí sa" zo šetriaceho režimu si vždy pýtať užívateľské heslo

Autor:
Henrich Ľubomír Proksa ©