Windows 7 Hardening Guide

Návod na bezpečnú konfiguráciu OS Windows 7

Príručka administrátora

Autor: CSIRT.SK

Dátum vydania: 28.10.2014
Verzia: 1

CSIRT.SK
www.csirt.gov.sk

Windows 7 Hardening Guide

1 Všeobecné informácie

Rozsah tejto príručky sa zameriava na operačný systém Windows 7, konkrétne verziu Windows 7 Enterprise. Venuje sa základnej konfigurácií zabezpečení operačného systému, siete, služieb a aplikácií.

1.1 Zoznam definícií

OS - Operačný Systém;

PC – *Personal Computer*, počítač; zariadenie, ktorého hardening vykonávame;

doména – spojená skupina počítačov a prístrojov, ktoré podľa adresy IP resp. doménového mena patria do rovnakej časti siete;

služba (service) – v kontexte systémov Windows NT je službou program, spustený na pozadí systému; ide o analógiu k démonovi v prostredí UNIX;

whitelist - spôsob kontroly prístupu, ktorý zakazuje všetky vstupy okrem vyslovene povolených;

blacklist - spôsob kontroly prístupu, ktorý povoľuje všetky vstupy okrem vyslovene zakázaných;

malware – všeobecné označenie škodlivého softvéru; patria sem napr. červy, trójske kone, adware, spyware a pod.

1.2 Ako používať túto príručku

Táto príručka slúži ako zoznam odporúčaní, ktoré je vhodné aplikovať aby sa znížilo riziko úspešného útoku na daný systém. Je napísaná pre všeobecné použitie. Príručku odporúčame použiť tak, že sa aplikujú potrebné úpravy zo všetkých sekcií. Poradie vykonania a voľba opatrení závisí na parametroch systému, požadovaného stupňa zabezpečenia a prostredia, v ktorom je stanica umiestnená. Opatrenia, vzťahujúce sa iba na určité systémy (napr. PC pripojené v doméne) či funkcie, požadované od zariadenia, sú príslušne popísané. Pri väčšine opatrení uvádzame zdôvodnenie ich použitia, riziká plynúce z ich chýbajúcej implementácie ako aj postup ich zavedenia. Postup aplikácie niektorých opatrení je však obsiahly, resp. líši sa medzi verziami aplikácií, na ktoré sa vzťahujú či od požiadaviek na systém. V týchto prípadoch preto uvádzame základnú myšlienku a cieľ konkrétneho bodu hardeningu, presný postup a voľbu nástrojov na jeho dosiahnutie ponechávame na administrátora.

Každé odporúčanie je označené na stupnici dôležitosti od 1 (najnižšia dôležitosť) až po 3 (najvyššia dôležitosť). Dôležitosť súvisí s požadovanou úrovňou zabezpečenia systému:

> **Stupeň 1** : Opatrenia, ktoré sa odporúča aplikovať na systémy s požadovanou vysokou úrovňou bezpečnosti.
>
> **Stupeň 2**: Opatrenia pre systémy, vyžadujúce zvýšenú úroveň bezpečnosti.
>
> **Stupeň 3**: Aplikovať zmeny označené úrovňou 3 sa odporúča na všetkých systémoch.

1.3 Hardening

Aplikácie ako webové servery, poštové servery alebo rôzne operačné systémy sú určené na mnohé činnosti a do mnohých prostredí. Často sa nevyužívajú všetky funkcie týchto aplikácií, avšak ich

funkcionalita je stále dostupná. To rozširuje tzv. *attack surface* (kód, ktorý môže vykonať aj neautorizovaný používateľ, ide teda o všetky prístupové body programu) aplikácie, čo priamo zvyšuje riziko napadnutia aplikácie (systému).

Cieľom hardeningu je zredukovať zraniteľnú plochu aplikácií bezpečnou konfiguráciou, aby boli robustnejšie a odolnejšie voči útokom. Spočíva v odstránení množstva zraniteľných bodov z aplikácie blokovaním častí programov, ktoré nie sú potrebné, prípadne obmedzení funkčnosti určitých častí programu. V dôsledku toho je systém (resp. aplikácia) omnoho odolnejší voči útokom.

Odporúčané konfigurácie sa menia podľa aplikácií, v závislosti od verzií operačných systémov, na ktorých sú aplikácie spustené a aj verzií inštalovaných aplikácií.

1.4 Všeobecné princípy

Všeobecným princípom hardeningu je minimalizovať miesta, o ktoré by sa útočník mohol zachytiť pri počiatočných fázach útoku.

Takéto všeobecné princípy sú:

- Šifrovanie všetkej citlivej komunikácie
- Spúšťanie iba nevyhnutných aplikácií
- Rozloženie služieb na odlišné servery
- Prideľovanie minimálnych potrebných prístupových práv – tzv. princíp *Least privilege*
- Časté aktualizácie
- Blokovanie nepotrebných častí (systému, programov)
- Použiť whitelist namiesto blacklistu
- Zabezpečenie prístupovej siete (IDS, IPS)
- Detekcia škodlivého softvéru (antivírus, kontrola na prítomnosť rootkitov, ...)
- Auditné záznamy (ukladanie a analýza)

Na základe týchto pravidiel boli odvodené odporúčané konfigurácie, ktoré mnohonásobne sťažujú neoprávnený prienik do systému, prípadne eskalovanie prieniku na prevzatie kontroly nad systémom.

2 Používatelia

Systém je potrebné využívať pod používateľom ktorý má len používateľské práva. Ide o dodržanie princípu *Least Privilege,* teda najnižších oprávnení. Ak totiž dôjde k úspešnému útoku na nejaké konto, útočník získa práve také oprávnenia, aké ku kompromitovanému kontu prislúchali.

Poznáme nasledovné stupne prístupových oprávnení:

- **User** – poskytuje prístup na spúšťanie aplikácií a použitie základných funkcií systému;
- **Power User** – pre používateľov, ktorí vyžadujú väčší vplyv na riadenie systému, nepotrebujú však neobmedzené oprávnenia;
- **Administrator** – práva administrátora majú používatelia zodpovední za inštaláciu HW a SW a spravujúci systém;
- **System** alebo **Local System** – najvyšší stupeň prístupových oprávnení, vyhradený pre služby a systémové funkcie bežiace na najvyššej úrovni prístupu k správe oblastí operačného systému, ktoré sú počas štandardnej práce chránené. Spustenie služby pod kontom lokálneho systému oddeľuje činnosť používateľa od operačného systému.

V prípade, že by k útoku došlo počas toho, ako sme prihlásený ako administrátor, útočník by získal všetky jeho práva, vrátane práv umožňujúcich inšlalácie nových programov, formátovanie diskov či vykonávanie iných zmien v systéme. Preto sa ako administrátor či systémový používateľ prihlasujeme len v najnutnejších prípadoch. Pri kompromitácií konta bežného používateľa síce možno jeho práva eskalovať, útočníkovi to však minimálne zaberie istý čas. Počas neho je šanca narušenie detegovať a prienik do systému včas ošetriť.

3 Konfigurácia systému

3.1 Nastavenie UAC – User Account Control

Stupeň 3

Postup:

1. V sekcií *Ovládací panel\Systém a zabezpečenie*, v oddiele *Centrum akcii* kliknúť na *Zmeniť nastavenie kontroly používateľských kont*

2. Nastavenie na voľbu *Vždy upozorniť*

Dôvod:

Kontrola používateľských kont (*UAC*) upozorňuje používateľa pred vykonaním zmien v počítači, ktoré vyžadujú povolenie na úrovni správcu. V predvolenom nastavení kontrola používateľských kont upozorňuje, keď programy vykonávajú zmeny v počítači, no môžete určiť, ako často vás má upozorňovať.

Na moderných verziách Windows bežia aplikácie bez akýchkoľvek administrátorských práv. Majú rovnaké prístupy ako štandardný používateľ, preto nemôžu vykonávať zmeny na OS, súborovom systéme alebo na nastavení registrov. Takisto nemôžu modifikovať nič, čoho vlastníkom je iný používateľ. Aplikácie môžu meniť len ich vlastné súbory a nastavenia registrov.

V prípade, že používateľ nemá práva administrátora (a to by mať nemal), je vždy oboznámený o vykonávaní zmien na PC. V prípade, že sa snažil o inštaláciu softvéru potrebného na prácu, musí sa obrátiť na administrátora. Ten má priestor zvážiť, či je inštalácia nevyhnutná, alebo by mohla predstavovať bezpečnostné riziko. V prípade, že používateľ zamýšľal inštalovať nepovolený softvér, nesúvisiaci s predmetom jeho činnosti, nedostatočné oprávnenie ho od úmyslu môže odradiť.

V prípade, že užívateľ je administrátorom, je takisto upozornený, že bude na PC vykonávať zmeny. Zabraňuje sa tak nezámernému spusteniu inštalácie napr. kliknutím na nesprávny odkaz alebo spustení skriptu, umiestneného na infikovanej stránke. Bežný používateľ by pri neočakávanom upozornení na vykonávanie zmien mal administrátora upozorniť, môže totiž ísť o cielený pokus o útok. Po aplikácií bezpečnostných šablón bude potrebné pri každom zobrazení UAC dialógu zadať aj heslo, aby sa predišlo neúmyselnému spusteniu neuatorizovanej akcie.

Tým, že aj zmena súborov iných používateľov vyžaduje administrátorské práva, UAC upozorní, ak by používateľ išiel omylom prepísať/zmazať cudzie súbory - mohol sa nechtiac dostať do cudzieho priečinka, ktorý nebol chránený kontrolou prístupu.

Možné dôsledky, ak opatrenie neaplikujeme :

Administrátor nie je upozornený na vykonávanie zmien v systéme. Na pozadí sa tak môžu inštalovať a inštalovať neautorizované potenciálne škodlivé aplikácie bez toho, aby si to všimol. Bežný používateľ síce nemá oprávnenie na inštaláciu, mohol by však podstrčený SW spustiť, čo môže viesť k škodám.

3.2 Zapnutie automatických aktualizácií

Stupeň 3

Zapnutia automatických aktualizácií zabezpečí aktualizáciu softvéru od Microsoft.

Zapnutie automatických aktualizácií je možné prostredníctvom doménovej politiky:

Ovládací panel\Systém a zabezpečenie\Windows Update\Zmeniť nastavenie

Dôvod:

Aktualizácie SW od Microsoft riešia novoobjavené zraniteľnosti systémov a aplikácií spoločnosti Microsoft. Inštaláciou Updates ich proti známym hrozbám chránime. Stále sa objavujú nové zraniteľnosti, dovtedy neznáme a ešte stále zneužiteľné. Preto je v záujme každého administrátora zabezpečiť systém najlepšie, ako je aktuálne možné. Automatické aktualizácie tomu výrazne dopomáhajú.

Možné dôsledky, ak opatrenie neaplikujeme :

Neaktualizovaný systém nie je chránený ani proti tým zraniteľnostiam, ktoré boli odhalené a ošetrené.

3.3 Konfigurácia AppLockera

Stupeň 3

AppLocker funguje iba na verziách Windows 7 Enterprise.

Postup:

1. Ako prvé spustíme služby ako administrátor:

EN: *Start button/Control Panel/System and Security/Administrative Tools/Services*

SK: *Štart/Ovládací panel/Systém a zabezpečenie/Nástroje na správu/Services*

2. Zapnúť službu *Application Identity* a nastaviť ju na *Automatic.* Táto služba určuje a overuje identitu spúšťanej aplikácie. Ak by nebola spustená, uplatnenie *AppLockera* by nebolo možné.

3. Vytvorenie defaultných politík je možné prostredníctvom lokálnej politiky v časti *AppLocker*.

Konfigurácia Počítača\Nastavenie Systému Windows\Security Settings\Application Control Policies\AppLocker.

Do vyhľadávača Windows zadáme Local Security Policies, ktoré spustíme ako správca. Klikneme pravým tlačidlom myši na AppLocker a vyberieme položku Vlastnosti:

- Panel *Advanced*
  - Zaškrtnúť *Enable DLL rule collection*
- Panel *Enforcement*

- Zaškrtnúť *Configured* a vybrať *Enforce rules* v častiach
  - *Executable Rules*
  - *Windows Installer Rules*
  - *Script Rules*

Konfigurácia pravidiel: Vytvoríme defaultné pravidlá každej triedy, t.j.

- *Executable Rules - Create Default Rules*
- *Windows Installer Rules - Create Default Rules*
- *Script Rules - Create Default Rules*

Pravidlá konfigurujeme nasledovne: Vľavo na paneli *AppLocker*-a postupne rozklikávame podzáložky *Executable, Windows Installer* a *Script rules*, aby sa vpravo objavil prázdny panel. Naň zakaždým klikneme pravým tlačidlom myši a zvolíme *Create default rules.* Objavia sa 3 nové pravidlá pre každú triedu.

Executable Rules povoľujú spúšťanie súborov uložených v priečinkoch *Program Files* a *Windows* všetkým používateľom. Tretie pravidlo povoľuje administrátorovi spúšťanie všetkých súborov. *Installer Rules* povoľujú neobmedzenú inštaláciu súborov so signatútou Windows inštalátora a súbory v priečinku *Windows/Installers*. Administrátor môže spustiť windowsové inštalátory bez ohľadu na ich umiestnenie. Defaultné *Script Rules* obmedzujú používateľa na skripty z *Program Files* a *Windows*. Administrátor môže používať všetky skripty.

4. Vytvorenie výnimky z pravidla:

- pravým tlačidlom klikneme na pravidlo a zvolíme *Vlastnosti*.
- V záložke *Exceptions* vyberieme typ výnimky (resp. typ podmienky, na základe ktorej bude pravidlo a výnimka z neho vytvorená) – *Publisher*, *Path* alebo *File hash*.

Napr. Po požiadavke na vytvorenie defaultných Executable rules bolo pridané pravidlo, ktoré povoľuje všetkým používateľom spúšťať súbory uložené v priečinku Windows. Z tohto pravidla môžeme vytvoriť Path výnimku pre priečinok C:\Users\palo - z tohto priečinka bude potom takisto možné spúšťať súbory. Pri Publisher exception vyberieme súbor so SW a nastavíme filter podľa vydavateľa SW, mena produktu, mena súboru či dokonca verzie súboru, na ktorú sa pravidlo nevzťahuje. Pri vytváraní File Hash exception opäť vyberáme vykonateľný súbor, ktorého hash určuje jeho vylúčenie z pravidla. Postup je rovnaký pre WinInstaller pravidlá, iba vyberáme Windows Installer súbory, pre Script Rules zase súbory skriptov.

Dôvod:

AppLocker povoľuje a zakazuje spúšťane aplikácií a skriptov na základe implementovaných politík. Umožňuje administrátorovi kontrolu nad tým, aké aplikácie môžu používatelia spúšťať. Jeho použitie je efektívne v organizáciách s jednoduchou štruktúrou, kde sú ciele obmedzení jednoznačné. Vo veľkých organizáciách, ktoré kladú dôraz na vysoký stupeň kontroly nad ich zariadeniami s pomerne malým počtom aplikácií, je *AppLocker* takisto vhodným riešením. Implicitne pracuje v *Allow List Mode* režime.

To znamená, že budú povolené iba tie aplikácie, ku ktorým bolo vytvorené zodpovedajúce pravidlo. Preto s rastúcim počtom kontrolovaných aplikácií rastú náklady na riadenie a správu politík.

AppLocker riadi štandardné spustiteľné súbory, inštalátory Windowsových aplikácií a DLL súbory. Umožňuje definovať pravidlá na správu súborov na základe ich signatúry (typ a názov súboru, vydavateľ, meno či verzia produktu....) Vytvorené pravidlá možno aplikovať separátne na rôzne skupiny používateľov, podľa predmetu ich činnosti, stupňa citlivosti aplikácie a pod. Tak zabezpečíme, že napr. aplikáciu môžu spúšťať len oprávnené osoby či iba administrátor/konkrétny používateľ. Bežnému používateľovi tak nebude povolené spúšťať napríklad tzv. portable aplikácie, ako napr. torrenty, prehliadače a pod. Z pravidiel možno prideliť výnimku. Tak môže admin zabezpečiť vyšší stupeň bezpečnosti, než umožňuje samotné obmedzenie práv bežného používateľa.

Možné dôsledky, ak opatrenie neaplikujeme :

Používatelia môžu spúšťať aplikácie, ku ktorým nemajú mať prístup, resp. môžu spúšťať prenosné aplikácie. Bezpečnostné riziko je spojené s tým, že aj bežný používateľ môže aplikácie spúšťať, hoci nemá dostatočné práva na inštaláciu. Stačí poslať mail s infikovaným odkazom a zmanipulovať používateľa, aby prilinkovanú stránku navštívil. Tak sa malware automaticky spustí a môže spôsobiť škody v systéme, hoci ho používateľ pre nedostatočné oprávnenia neuložil do ProgFiles.

3.4 Software Restriction Policy

Stupeň 3

Software Restriction Policy (SRP) je predchodca *AppLockera*. Kým *AppLocker* funguje na podporovaných platformách Windows Server 2012, Windows Server 2008 R2, Windows 8 a Windows 7, SRP poskytuje podobnú funkcionalitu na starších systémoch od Windows Server 2003 a Windows XP. Obe technológie pre manažment v doméne používajú *Group Policy*. Ak obe implementujeme v rovnakej doméne, na *AppLocker*-kompatibilných staniciach má politika *AppLockera* prednosť pred politikami *SRP*.

Funkcie *SRP* a *AppLockera* sú v niektorých ohľadoch rozdielne. *AppLocker* nepodporuje pridávanie iných typov súborov (okrem prednastavenej sady), na ktoré sa majú vzťahovať nejaké obmedzenia. SRP síce neumožňuje vytvorenie pravidla typu *Publisher*, pozná ale typ *Signature* a *Internet Zone*. Pravidlá *SRP* sa uplatňujú na všetkých používateľov PC a nemožno z nich udeľovať výnimky. *AppLocker* umožní výnimky vytvárať, exportovať a importovať politiky a aplikovať pravidlá na konkrétneho používateľa alebo ich skupinu.

SRP môže byť, podobne ako AppLocker, konfigurovaná na prácu v režime *Allow List Mode*. Primárne ale funguje v móde *Deny List Mode.* Vtedy sú zakázané iba aplikácie, ku ktorým boli vytvorené takéto pravidlá. Ostatné programy sú povolené.

Postup:

1. EN: *Control Panel/Administrative Tools/Local Security Policy/Software Restriction Policy.*

SK: *Ovládací panel/Systém a zabezpečenie/Nástroje na správu/Local Security Policy/Software Restriction Policy*.

Pravé tlačidlo myšky > *New Software restriction policy*

2. Dvojklik na *Designated File Types*. Nájdeme *LNK* príponu (ide o skrytú príponu Odkazov (Shortcuts) a klikneme na *Remove* button (Dôležité!!!). Následne zadáme nasledujúce prípony, vždy po jednej. Po každej stlačíme tlačidlo *Add*, aby sme ju pridali do zoznamu:

vbs, js, jse, otf, sct, shb, vbe, wsf, wsh

3. Rozklikneme záložku *Enforcement* - vyberieme *All software files* (tak do zoznamu zahrnieme aj DLL súbory)

4. Rozklikneme *Additional Rules*, pravým tlačidlom na pravý panel, vyberieme *New Path Rule* a zadáme cestu *C:\Program files (x86).* Zvolíme *Security Level: Unrestricted*. To znamená, že z tohto priečinka môžu byť spúšťané všetky súbory.

Obdobne pridáme nasledovné pravidlá pre cesty, s bezpečnostným levelom *Disallowed* – Zakázané. Tým zakážeme spúšťanie aplikácií z nasledovných priečinkov:

C:\windows\debug\WIA

C:\windows\Registration\CRMLog

C:\windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}

C:\windows\System32\com\dmp

C:\windows\System32\FxsTmp

C:\windows\System32\spool\PRINTERS

C:\windows\System32\spool\drivers\color

C:\windows\System32\Tasks

C:\windows\SysWOW64\com\dmp

C:\windows\SysWOW64\FxsTmp

C:\windows\SysWOW64\Tasks

C:\windows\Tasks

C:\windows\Temp

C:\windows\tracing

Dôvod:

Ak je *Software Restriction Policy* aktivovaná, bráni v behu všetkých programov okrem tých, ktoré sú uložené v *Program Files* alebo *Windows*. To znamená, že akýkoľvek malware stiahnutý do priečinka *Temporary Internet Files* či inde nebude spustený. Prehliadače a pluginy mávajú také zraniteľnosti,

ktoré umožňujú infikovaným stránkam vynútiť stiahnutie. Keďže počítače bývajú požívané štandardnými používateľmi, malware nemôže byť nainštalovaný do žiadneho z vyššie uvedených 2 priečinkov. Na to sú totiž potrebné oprávnenia na úrovni administrátora. Tým pádom je stroj chránený pred behom nechcených programov. Ak sa navyše s PC delíme s inými používateľmi, máme istotu, že nemôžu na stroj inštalovať programy či akýmkoľvek spôsobom systém modifikovať.

Možné dôsledky, ak opatrenie neaplikujeme :

Bežný používateľ by mohol spúšťať všetko, napríklad malware maskovaný ako *.vbs* skript, poslaný v prílohe e-mailu z navonok dôveryhodnej stránky. Takisto môže spúšťať programy, na ktoré podľa (zle implementovanej) business logiky nemá právo.

3.5 Vypnutie nepotrebných služieb

Stupeň 3

Postup:

EN: *Start button/Control Panel/System and Security/Administrative Tools/Services*

SK: *Štart/Ovládací panel/Systém a zabezpečenie/Nástroje na správu/Services*

Pravým tlačidlom klikneme na nasledujúce služby (*Services)*. Vyberieme *Vlastnosti* a nastavíme *Startup Type* na *Disabled*. Služby tak nebudú pri zapnutí PC automaticky aktivované. Ak nastavíme možnosť *Manual*, služba bude spustená, ak tak spraví program alebo iná bežiaca služba. *Automatic* spôsobí automatické spustenie služby po bootovaní PC.

Služba	Konto	Cieľový stav	Popis
BranchCache	Network Service	disabled	Ukladá dáta zo serverov vzdialených pracovísk. Keď jeden z klientov na lokálnej pobočke žiada o takéto dáta, zostanú uložené buď na lokálnom serveri, alebo na jeho stanici – ak má *BranchCache* zapnutý. Keď o ten istý obsah požiada iný klient pobočky, nebude opäť sťahovať dáta zo vzdialeného servera cez WAN, ale z lokálneho klienta či servera, kde sú nacacheované.
Computer Browser	System	Manual/ disabled	Udržiava zoznam zariadení a zdrojov v sieti. V doménovej alebo pracovnej sieti je používaná na prehliadanie siete či mapovanie zdieľaných priečinkov. Aj tam však nemusí bežať na všetkých PC, iba tých, ktoré sú nakonfigurované ako prehliadač.
Distributed Link Tracking Client	System	disabled	Spravuje linky medzi *NTFS(New Technology File System)* súbormi na PC alebo medzi PC v (doménovej) sieti, napr. aby sa dalo k

			súboru stále pristúpiť, aj keď bol presunutý či premenovaný.
DNS Client	Network Service	automatic	Ukladá predtým vyhľadávané doménové mená a registruje plné meno PC, na ktorom beží; býva cieľom cache poisoningu; ak ho vypneme, služby na ňom závislé prestanú fungovať a rýchlosť surfovania sa zníži (záznamy sa budú musieť zakaždým resolvovať).
Function Discovery Provider Host	Local Service	Manual/ disabled	Hostuje *Function Discovery (FD)* poskytovateľov *network discovery*. Títo FD poskytovatelia zabezpečujú služby objavenia siete protokolom *Simple Services Discovery Protocol (SSDP)* a *Web Services – Discovery (WS-D)*. Podporný servis pre *HomeGroup*, viď nižšie.
Function Discovery Resource Publication	Local Service	Manual/ disabled	Opäť súvisí aj s *HomeGroup*; oznamuje prítomnosť PC a s ním spojených zdrojov, takže sú viditeľné na sieti. Po vypnutí servisu sa sieťové zdroje nebudú dať objaviť z iných PC na sieti.
HomeGroup Listener	System	Manual/ disabled	Spôsobí, že zmeny lokálneho PC budú spojené s konfiguráciou a správou PC pripojeného k *HomeGroup* či domácej sieti. *HomeGroup* je nový nástroj na zdieľanie súborov vo Win7; všetky zdieľané dáta siete sú zabezpečené jediným heslom. Toto je jedným z dôvodov, prečo je služba považovaná za rizikovú. Ak neplánujeme *HomeGroup* používať, mali by sme všetky jej komponenty a podporné služby deaktivovať.
HomeGroup Provider	System	Manual/ disabled	Vykonáva sieťové úlohy spojené s konfiguráciou a správou *HomeGroup*.
Internet Connection Sharing	System	disabled	PC sa navonok správa ako router, poskytuje NAT, adresovanie, preklad mien a /alebo *Intrusion Prevention Services* pre domáce a malé pracovné siete.
IP Helper	System	disabled	Zabezpečuje IPv6 tunneling. Prečo vypíname IPv6 súčasti, vysvetlíme nižšie.
Link Layer Topology Discovery Mapper	Local Service	Manual/ disabled	Tvorí mapu siete, do ktorej je stroj pripojený; pre domáci PC alebo PC pripojený do domény nemá služba využitie. SK: *Mapovač zisťovania topológie úrovne vrstvy prepojení*
Media Center Extender Service	Local Service	disabled	Mení PC na multimediálny server, Media Extendery sa naň budú môcť pripojiť. Ak nie je nevyhnutná, službu vypíname.

			SK: *Služba Media Center Extender*
Net. TCP port Sharing Service	Local Service	disabled	Umožňuje zdieľanie TCP portov pomocou protokolu *Net.TCP*. Na samostatných a domácich staniciach by vôbec nemal byť nainštalovaný- na *Windows 8* už medzi predinštalovanými službami nie je.
NetLogon	System	manual	Služba nie je na samostatných PC alebo PC v domácej skupine nevyhnutná, tam ju možno vypnúť. Je však podmienkou na pripojenie sa k doménovému radiču. Udržiava totiž zabezpečený kanál na autentifikáciu používateľov a služieb medzi PC a radičom. Ak servis vypneme, PC možno používateľov neautentifikuje a radič nezaregistruje DNS záznamy. Preto ak je zariadenie pripojené do domény, službu nevypíname.
Network Access Protection Agent	Network Service	Manual/ disabled	Zbiera a reportuje bezpečnostnú konfiguráciu lokálnych zariadení. Ak by nezodpovedala nastaveným politikám, môžu mať stroje obmedzený prístup k sieti, kým nebudú updatované. Aktualizované môzu byť aj automaticky. Ak neplánujeme pomocou nej kontrolovať stav PC v doméne, môžeme službu vypnúť, rovnako ako na samostatnom PC.
Offline Files	System	disabled	Správa *Offline Files.* Odpovedá na prihlásenia/odhlásenia a iné udalosti a odosiela o nich správy zariadeniam, ktoré o ne majú záujem. Takéto správanie je z bezpečnostného hľadiska nežiadúce. Ak nesynchronizujeme súbory medzi počítačmi, mali by sme túto službu vypnúť. Ak je zariadenie pripojené do domény, službu ponechávame aktívnu.
Parental Controls	Local Service	disabled	Ponechané pre kompatibilitu s *Windows Vista*. Ak nepotrebudeme rodičovskú kontrolu, službu vypíname.
Peer Name Resolution Protocol	Local Service	disabled	Umožňuje resolvovanie mien medzi peermi bez servera, cez *PNRP* protokol. Je potrebný pre beh služieb *Remote Assistance* a *HomeGroup*, ktoré z bezpečnostných dôvodov deaktivujeme. Preto servis aj ďalšie s ním spojené služby (*PN Grouping, PNRP Machine Name Publication Service, PN Identity Manager*) vypíname.
Peer Networking Grouping	Local Service	disabled	Podporná služba pre *HomeGroup* a *Remote Assistance*, preto ju tiež deaktivujeme.

Peer Networking Identity Mgr	Local Service	disabled	Podporná služba pre *HomeGroup* a *Remote Assistance.*
Performance Counter DLL Host		disabled	Povoľuje dopyty na počítadlá výkonu od vzdialených používateľov a 64-bitových procesov. Nie je žiadúce, aby PC na obdobné požiadavky odpovedal, preto servis vypíname.
Performance Logs & Alerts	Local Service	disabled	Zber dát o výkone lokálnych i vzdialených staníc na základe prekonfigovaných parametrov, ich zápis do logov či spustenie alarmu. Spôsobuje overhead, prínos je zanedbateľný. Preto službu vypneme. Navyše pre svoju funkciu vyžaduje *RPC*, pozri nižšie.
PnP-X Ip Bus Enumerator	System	manual	Spravuje zbernicu virtuálnych sietí. Používa *SSDP* na vyhľadanie pripojených zaradení a priraďuje ich do *PnP.* Využívajú to napr. Media Extendery, ktoré zakazujeme, preto netreba ani túto službu.
PNRP Machine Name Publication Service	Local Service	manual	Server odpovedajúci menom stroja, na ktorom beží, komunikácia *Public Name Resolution Protocol*-u. Vyžaduje IPv6, ktorú vypíname, služba teda nepobeží.
Quality Windows Audio Video Experience	Local Service	disabled	Multimediálny server, sieťová platforma pre Audio Video (AV) streaming aplikácie na domácich IP sieťach. Podporuje výkon a spoľahlivosť AV streamovania zabezpečením QoS pre AV aplikácie. Má mechanizmy pre riadenie prístupu, prioritizáciu prevádzky a pod. Ak nie je služba nevyhnutná, vypíname ju.
Remote Access Auto Connection Mgr	System	disabled	Vytvorí spojenie k vzdialenej sieti kedykoľvek program odkazuje na vzdialené *DNS* alebo *NetBIOS* meno či adresu. Potrebné pre DSL, dial-up či káblové pripojenia k internetu. Ak však používame hardvérový gateway alebo router, servis nie je potrebný.
Remote Access Connection Manager	System	Manual/ disabled	Spravuje pripojenie cez dial-up a VPN, ktoré požadujú prihlasovanie. Vtedy nastavujeme typ *Manual,* musíme však spustiť aj ďalšie služby: *Telephony (PnP a RPC)* a *Secure Socket Tunneling Protocol Service*. Ak na prístup k Internetu používame HW gateway alebo router, servis nie je potrebný.
Remote Desktop Configuration (RDCS)	System	Manual/ disabled	Zodpovedá za všetky *Remote Desktop* služby a s nimi spojené konfigurácie a aktivity na správu relácií, ktoré vyžadujú System kontext. Ak je potrebné ponechať k stanici možnosť vzdialeného prístupu, nastavíme *Manual*, v opačnom prípade *Disabled*.

Remote Desktop Services	Network Services	Manual/ disabled	Povoľuje používateľom interaktívne spojenie so vzdialeným PC. Ak je potrebné ponechať používateľovi/administrátorovi možnosť vzdialeného prístupu, nastavíme *Manual*, v opačnom prípade *Disabled*. Služby *Remote Desktop* a *Remote Desktop Session Host Server* sú na ňom závislé, preto ich takisto vypíname.
Remote Desktop Service UserMode Port Redirector	System	Manual/ disabled	Umožňuje presmerovanie tlačiarní, ovládačov a portov pre RD spojenia. Ako vidíme, na bežných používateľských PC všetky služby súvisiace so *Vzdialeným pripojením* z bezpečnostných dôvodov zakážeme. Nie je žiadúce, aby bol k stanici umožnený vzdialený prístup. Ak má byť prístupmožný, napr. kvôli administrácií, služby nastavujeme na *Manual*. V takom prípade je nevyhnutný ďalší hardening všetkých súčastí *Remote Desktop* služby.
Remote Registry	Local Service	disabled	Umožňuje cudzím PC meniť registre. Jedna zo služieb, ktorú by sme mali na domácej sieti kvôli zabezpečeniu vypnúť.
Routing and Remote Access	System	disabled	Povoľuje PC dial-in na lokálny stroj cez modem či iné zariadenie a tak pristúpiť na lokálnu sieť, či už štandardne, alebo cez VPN. Ak na pripojenie k Internetu používame HW FW/gateway/router, nepoužívame *IPsec* ani *InternetConnectionSharing*, túto službu vypíname (a s ňou aj ďalšie: *Base Filtering Engine*, *IKE and AuthIP IPsec Keying Modules, Internet Connection Sharing (ICS), IPsec Policy Agent, Routing and Remote Access*, prípadne dokonca *Windows Firewall*)
Secondary Logon	System	disabled	*SK: Sekundárne prihlásenie*; Umožňuje prihlasovanie s alternujúcimi právami. To značí, že dovoľuje bežnému prihlásenému používateľovi prihlásiť sa ako správca či iný používateľ, teda s vyššími oprávneniami, aké prislúchajú primárnemu loginu; službu vypíname kvôli automatizovaným útokom, kedy sa útočí na konto bežného používateľa a cez neho sa eskaluje na konto s vyššími oprávneniami. Rovnako sa môže stať, že privilegovaný používateľ spustí aplikáciu pomocou konta s nižšími právami. So sekundárneho prihlasovania teda plynú zrejmé riziká, preto ho neumožňíme a službu vypíname.
Secure Socket	Local	disabled	Podpora protokolu *SSTP* na pripojenie k vzdialeným PC cez *VPN*. Ak

Tunneling Protocol Service	Service		nepoužívame *VPN*, *ICS* a náš poskytovateľ nepožaduje prihlasovanie sa, službu vypíname.
Server	System	disabled	Na sieti na stanici, kde server beží, podporuje zdieľanie SMB súborov, tlače a pomenovaných rúr. Súvisí s vypínanými službami *HomeGroup*, *File and Printer Sharing*. Jedna z najzraniteľnejších služieb, na ktorú sa najviac útočí. Vypnutím prídeme o viaceré funkcie, napr. zdieľanie súborov a diskov, ale väčšie riziká plynú zo zapnutého servera.
SNMP Trap	Local Service	disabled	Prijíma trap správy od lokálnych alebo vzdialených *SNMP* agentov a preposiela ich *SNMP* managerovi, spustenom na PC. Normálne nepotrebudeme *SNMP* trapy, nie je preto dôvod na prevádzku servisu. Rizikom je, že sa niekto za agenta môže vydávať a podstrčí nepravdivý či škodlivý trap. Napr. Trap označí stanicu za nefunkčnú, hoci to tak nie je ap.
SSDP Discovery	Local Service	disabled	Deteguje poprepájané zariadenia a služby na sieti, ktoré používajú *SSDP* protokol, napr. *UPnP* zariadenia. Takisto ale oznamuje *SSDP* zariadenia a služby bežiace na našom zariadení. Potrebné pre funkčnosť *UPnP* a *Media Center.* V prípade, že ich nepoužívame, službu vypneme.
Tablet PC Input Service	System	disabled	Umožňuje použitie *Tablet PC pen and ink*. Ak nevyhnutne nepoužívame tablet, servis vypíname.
TCP/IP NetBIOS Helper	Local Service	disabled	Preklad *NetBIOS* mien, nutný pre zdieľanie prostriedkov na sieti. Viď ďalší postup – *NetBIOS* nad TCP/IP budeme vypínať. Ak je zariadenie pripojené do domény, službu ponechávame aktívnu.
Telephony	Network Service	disabled	Poskytuje *Telephony API* pre programy spravujúce telefonické spojenia. Závisí od neho dial-up, fax a niektoré VPN. Ak na prístup k Internetu používame HW gateway alebo router, servis nie je potrebný. Inak ponecháme režim *Automatic*. *SK: Telefonovanie*
UPnP Device Host	Local Service	disabled	Umožňuje hosting *UPnP* zariadení na PC. Nepotrebujeme *UPnP* => vypíname všetky súvisiace podporné služby.
Web Client	Local	disabled	Umožní windowsovým programom vytvárať, modifikovať a pristupovať k internetovým súborom. S výnimkou vývojárov

	Service		používajúcich *WebDAV* nemá používateľ dôvod mať túto službu aktívnu. Predstavuje bezpečnostné riziko.
Windows Connect Now	Local Service	disabled	Utilita na zjednodušenie konfigurácie WiFi pripojenia. Ak WiFi nemáme (napr. doménová sieť) alebo je náš poskytovateľ nekompatibilný s Windows 7, službu vypíname.
Windows Error Reporting Service	System	disabled	Reportuje problémy systému Microsoft-u a získava riešenia. Musíme zvážiť, či je nutné verejne informovať o našich problémoch. Zaberá to istý čas, prostriedky a prezrádza o nás informácie. Preto je službu lepšie vypnúť. Beží pod System kontom a komunikuje so sieťou.
Windows Event Collector	Network Service	disabled	Správa perzistentného odoberania správ o udalostiach zo vzdialených zdrojov, podporujúcich *WS-Management protocol*. Pre väčšinu bežných staníc to nie sú potrebné informácie, servis preto vypneme.
Windows Media Player Network Sharing Service	Network Service	disabled	Umožňuje zdieľanie WMP knižníc s ostatnými media playermi v sieti, ktoré používajú *UPnP*. Ak to nie je nevyhnutné, je to z bezpečnostných dôvodov nežiadúce. SK: *Windows Media Player – služba zdieľania v sieti*
Windows Remote Management	Network Service	disabled	Umožňuje vzdialený prístup cez shell, SW a HW konfiguráciu na diaľku. Zakázanie z bezpečnostných dôvodov.
WinHTTP Web Proxy Auto Discovery	Local Service	disabled	Implementuje klientský *HTTP* stack, poskytuje vývojárom istý typ http API na komunikáciu. Slúži na automatické objavenie proxy konfigurácie. Pre bežných používateľov nevyužitá služba.
WMI Performance Adapter	System	disabled	Poskytuje dáta o výkone nášho zariadenia iným PC, ktoré ich zbierajú; navyše pristupuje k sieti a beží pod kontom *System*, ktoré je útočníkmi cenené rovnako ako konto admininstrátora. Preto službu vypíname.
Workstation	Network Service	automatic	Vytvára a udržiava klientské sieťové spojenia so vzdialenými servermi pomocou *SMB* protokolu. Podobne ako služba *Server*, je nutná na zdieľanie súborov a tlačiarní na sieti. Závisí od nej služba *HomeGroup* a iné, ktoré sme deaktivovali. *Workstation* však nevypíname, je pre správny beh systému vitálna. Službu takisto

			nevypíname, ak je zariadenie pripojené do domény.

Pozn. ku Win Error Reporting:

Ak chceme tento servis vypnúť, treba zabezpečiť, aby sa pri automatickej aktualizácií systému opäť neaktivoval. Postup je nasledovný:

Ovládací panel/Systém a zabezpečenie/Centrum akcií. Údržba – pod *Vyhľadať riešenia na ohlásené problémy* otvoríme *Nastavenia.* Vyberieme *Nikdy nehľadať riešenia(neodporúča sa)*.

Dôvod:

Riadime sa princípom *"Čo nepotrebujeme, má byť vypnuté"*. Služby obsahujú zraniteľnosti, ktoré môže útočník zneužiť. Napr. *UPnP*, *Remote Registry* alebo služba *Remote Desktop* by nemali byť aktívne, pretože umožňujú vzdialené pripojenie na PC a vykonávanie zmien na ňom. Viaceré služby automaticky odosielajú informácie o stanici, iné zbytočne zaberajú čas procesora.

Množstvo služieb, ktoré bežne nepotrebujeme, beží pod účtom *System*. Prislúchajú im najvyššie možné oprávnenia. Ak útočník úspešne napadne systémovú službu, získa k PC prístup so systémovým účtom, ergo môže so strojom robiť prakticky čokoľvek. Navyše viaceré zo systémových služieb interagujú zo sieťou, sú teda otvorené komunikácií zvonka. Tým sú na útočenie ešte dostupnejšie. Preto akákoľvek nepoužívaná služba má byť vypnutá.

Možné dôsledky, ak opatrenie neaplikujeme :

Riskujeme napadnutie zraniteľnej služby a získanie vysokých práv útočníkom. Takisto vysielanie dát o výkone nášho PC alebo o na ňom bežiacich službách či reportovanie vzniknutých problémov nie je z bezpečnostného hľadiska ideálne. Vypnutím určitých služieb, napríklad *Server*, sa pripravíme o niektoré funkcie, užitočné napr. v pracovných sieťach. Vzhľadom na povahu služby je však výhodnejšie hľadať náhradné riešenie na zabezpečenie ňou vykonávanej funkcie, ako sa vystavovať rizikám, ktoré kvôli svojej zraniteľnosti prináša.

3.6 Vypnutie služby server

Stupeň 3

Postup:

Vypnúť službu server: *Services**Server*, pravé tlačidlo myši > *Stop*

Dôvod:

Na jednej strane nás to od viacerých služieb odstrihne, na druhej však ochráni pred množstvom útokov. Služba *Server* umožňuje pripojiť sa na stroj a zdieľanie súborov, z čoho plynie veľa možností zneužitia.

Možné dôsledky, ak opatrenie neaplikujeme:

Exploity mierené na službu Server. Napr. známy červ *Conflicker* využíval zraniteľnosť publikovanú v MS08-067 služby Server (2008-2009). Útočník nadviazal spojenie so stanicou iniciovaním SMB relácie

na porte 445/TCP obete. Ďalšou zraniteľnosťou Servera je CVE-2008-4250, súvisiaca s nesprávnym ošetrením špeciálne vytvorených RPC paketov. Obe zraniteľnosti umožňujú útočníkovi získať plnú kontrolu nad PC.

3.7 Vypnutie AutoPlay

Stupeň 3

Postup:

Ovládací panel/Hardvér a zvuk/Automatické prehrávanie. Pre každú položku vybrať *Nevykonať žiadnu akciu*. Takto ošetríme všetky používateľské účty.

Dôvod:

Zabránime automatickému prehrávaniu programov. Médiá vložené do PC, ako USB kľúče, môžu obsahovať malware. Je bezpečnejšie programy z externých médií prehrávať ručne.

Možné dôsledky, ak opatrenie neaplikujeme:

Riskujeme, že pri vložení kolegovho USB (napr. kvôli kopírovaniu súboru z neho) sa automaticky spustí malware, ktorým bol omylom(*alebo pre testovacie účely...) infikovaný.

3.8 Nastavenie logovania a Event Viewer

Stupeň 2

Dôvod a odporúčanie:

Významné udalosti, ktoré sa na PC udiali, sa zaznamenávajú do špeciálnych súborov – tzv. *Event logs*. Kedykoľvek nastane logovaná udalosť, napr. prihlásenie používateľa do systému, inštalácia nového softvéru či nastane chyba programu, záznam o tejto udalosti sa zapíše do logovacieho súboru. Výber a typ ukladaných informácií môže byť kľúčový pre uspech vyšetrovania v prípade vzniku incidentu. Logy sú významným podkladom pri forenznej analýze. Preto by sa konfigurácií logovania a auditu jeho výstupov mala venovať značná pozornosť.

Záznamy možno prezerať pomocou nástroja Windows EventViewer. Ten ukladá informácie dvoch kategórií do rôznych súborov:

- **Windows logs**
  - **Application logs** – záznamy o udalostiach v programoch, podľa závažnosti rozdelené na Chyby – *Errors* (vážne problémy, napr. strata dát), Varovania – *Warnings* (udalosť aktuálne nie veľmi závažná, ale s potenciálom spôsobiť problém v budúcnosti) a Info - *Information* (oznámenie o úspešnom vykonaní akcie programom, službou alebo ovládačom);
  - **Security** – inak nazávané aj auditné správy, môžu byť označené za úspešné *successful* alebo neúspešné *failed*, ako napr. prihlásenie používateľa do systému;
  - **Setup** – zariadenia konfigurované ako doménové radiče budú mať v tomto logu špecifické informácie;

- **System** – Záznamy o systémových udalostiach, zaznamenané systémovými službami a samotným OS; opäť kategorizované ako *Errors*, *Warnings* a *Information*;
- **Forwarded events** – udalosti z iných počítačov.

Logy týkajúce sa aplikácií a servisov sa rôznia.Obsahujú oddelené záznamy o bežiacich programoch aj detailnejšie logy špecifických služieb. Táto kategória sa preto ďalej člení na typy *Admin*, *Operational*, *Analytic* a *Debug* záznamy.

Veľmi dôležitou súčasťou práce administrátora systému je pravidelný audit logov. *Event Viewer* umožňuje zobraziť iba vybrané typy udalostí na základe nastaveného filtra.

Administrátor nastavuje, aké typy udalostí budú zaznamenávané pomocou *Local Security Policy/ Security Settings/Local Policies/Audit Policy*. Tak je možné zvoliť, ktoré udalosti si prajeme sledovať na akej úrovni a zamädziť tak tvorbe neprimerane veľkých a neprehľadných súborov. Rovnako je potrebné alokovať primeraný priestor pre záznamy (viď sekciu *Nastavenie Firewallu* – povoľujeme v nej logovanie udalostí a zväčšujeme vyhradené kapacity). Odporúčame nastaviť sledovanie *„Success, Failure“* pre *Audit account logon events, Audit account management, Audit logon events* a *Audit policy change*. *„Failure(Minimum)“* je postačujúce pre *Audit object access* a A*udit privilege use,* napokon *„Success(Minimum)“* pre *Audit system events* kategóriu. Vitálne pre prípad potreby auditu (napr. forenzná analýza) je nastaviť dostatočne veľký priestor pre bezpečnostný log tak, aby v ňom bolo možné uchovávať záznamy z minimálne 30 dní. Treba pritom zvážiť objem zaznamenávaných dát, ktorý systém generuje.

Naďalej však najdôležitejšou úlohou zostáva pravidelný audit logov.

3.9 Vypnutie rozhraní náchylných na DMA útok

Stupeň 1

Postup:

Vypnutie rozhraní a odinštalovanie ovládačov rozhraní a portov, ktoré nie sú používané. Vypnutie HW mapovania medzi rozhraním a pamäťou zariadenia. Zakázanie používania HW, kompatibilného s potenciálne zraniteľnými rozhraniami.

Dôvod:

Viaceré hardvérové rozhrania komunikujú pomocou priameho prístupu do pamäte (*Direct Memory Access*), bez zapojenia sa operačného systému. Zariadenia, ktoré sa do nich zapoja, budú napojené priamo na fyzický adresný priestor systému. DMA útok je typom útoku cez postranné kanály, kedy sa tieto expanzné porty zneužívajú na získanie prakticky neobmedzeného prístupu do systému. Ide napríklad o *FireWire* (rozranie IEEE-1394), *ExpressCard*, *Thunderbolt*, *USB*, *PCI* či *PCI Express*. V prípade, že tieto rozhrania nepoužívame, je preto odporúčané ich znefunkčniť.

Možné dôsledky, ak opatrenie neaplikujeme:

Riziko DMA útoku: Po pripojení sa k počítaču cez fyzické rozhranie útočník získa priamy prístup do pamäte. Tak môže obísť všetky bezpečnostné mechanizmy OS. Môže potom napríklad čítať šifrovacie

kľúče, inštalovať softvér či riadiť iné programy. Na útok stačí mať len fyzický prístup k zariadeniu. Existujú nastroje, pomocou ktorých možno DMA útok vykonať, napr. *Intrude* alebo *FinFireWire*.

3.10 Zabezpečenie IIS a MS SQL

Stupeň 3

Postup:

V závislosti od bezpečnostných požiadaviek a verzie *IIS* a *SQL* servera.

Dôvod:

Medzi obľúbené ciele útokov patria distribuované aplikácie. Medzi ne patria napríklad *Microsoft Internet Information Services – IIS*, či *MS SQL Server*. Nesú so sebou bezpečnostné riziká, preto je potrebné ich pred použitím dostatočne zabezpečiť.

Možné dôsledky, ak opatrenie neaplikujeme:

Známych je množstvo zraniteľností *IIS,* najmä u starších verzií (niektoré neboli nikdy ošetrené)*: IIS* servery boli v roku 2007 nositeľmi 49% svetového malware, hoci novšie verzie boli ošetrené lepšie.

4 Konfigurácia siete a firewallu

4.1 Základné nastavenia

Stupeň 3

Postup:

1. *Ovládací panel\Sieť a Internet – Zobraziť stav siete a sieťové úlohy – Lokálne pripojenie*.
2. Kliknúť tlačidlo *Vlastnosti* a odznačiť nasledujúce položky:
   - Client for MS Networks (vynechať pre zariadenia pripojené do domény)
   - File and Printer Sharing for Microsoft Networks
   - QoS Packet Scheduler
   - Link Layer Topology Discovery Mapper I/O Driver
   - Link Layer Topology Discovery Responder
   - Internet protocol version 6
3. Vybrať "*Internet Protocol version 4 (TCP IPv4)*", kliknúť na *Vlastnosti – Spresniť*,
   - v záložke "*DNS*" odznačiť "*Zaregistrovať adresy tohto pripojenia v systéme DNS*"
   - v záložke "WINS" vybrať "*Zakázať protokol NetBIOS nad protokolom TCP/IP*"

Dôvod:

Na to, aby nás útočník napadol zo vzdialenej stanice, musí interagovať s nejakým "u nás" bežiacim programom, ktorý pristupuje k sieti. Niektoré sieťové komponenty implementujú protokoly, ktoré môžu obsahovať zraniteľnosti. Čím viac protokolov je povolených, tým je riziko väčšie. Preto obmedzíme množstvo používaných protokolov na najnižšiu možnú mieru. Protokol, ktorý je v súčasnosti nevyhnutný na pripojenie do siete i na fungovanie väčšiny sieťových prvkov, je IPv4. Protokol IPv6 síce už dnes poskytuje viaceré zaujímavé možnosti, stále je však pomerne málo rozšírený a prakticky používaný. Preto zakazujeme protokol IPv6, ako aj všetky protokoly umožňujúce tunelovanie – prechod/mapovanie medzi verziami IPv4 a v6 v zmiešaných sieťach. Tunelovanie totiž obchádza zabezpečenie poskytované firewallmi. Tunelovaná IPv4 prevádzka sa totiž navonok javí ako IPv6, FW ju preto nechá prejsť bez kontroly obsahu.

Protokol *NetBIOS* (*Network Basic Input/Output System*) nad TCP/IP nie je nutný, pretože *NetBIOS* je aktívny aj bez tejto možnosti. Jeho vypnutie nad TCP/IP by ním generovanú prevádzku malo obmedziť na lokálnu podsieť.

Discovery protokoly slúžia na zmapovanie siete, aby sme získali prehľad o umiestnení zariadení a dostupných zdrojoch na sieti. Pre samostatné domáce stanice to význam nemá, sieť tvorí len PC a

router. Pre stroje zaradené do domény je táto služba vypnutá automaticky po ich pripojení k doméne.

File and Printer Sharing by malo byť zapnuté len pre prípad, že plánujeme nejaké adresáre alebo lokálne pripojené tlačiarne zdieľať. Aj v prípade zdieľania tlačiarní je rozumnejšie mať zariadenie s podporou pripojenia k sieti – sieťovú tlačiareň. Ak potom cez ňu útočník aj získa prístup do siete, bude to iba k tlačiarni, nie k PC.

Možné dôsledky, ak opatrenie neaplikujeme:

Ukrytie škodlivej IPv4 prevádzky pomocou IPv6 tunelovania. Viac aktívnych protokolov znamená viac zraniteľností, na ktoré možno útočiť. Existuje riziko, že útočník kompromituje privátnu sieť cez tlačiareň či zdieľané súbory.

4.2 Vypnúť nepoužívané TCP/IPv6 zariadenia a NETBT

Stupeň 3

Postup:

1. EN: *Control Panel / Device Manager, View menu / Show Hidden Devices*

- */Network*, zakázať *Wan Miniport IPv6*
- */Network*, zakázať *Microsoft ISATAP adapter (IPv6 tunnel)*
- */Network*, zakázať *Teredo Tunneling Pseudo Interface (IPv6 tunnel)*
- */Non-Plug and Play Drivers /Remote Access IPv6 ARP Driver > Properties* > záložka *Driver* >: zmeniť *Startup Type* zo *System* na *Disable*
- */Non-Plug and Play Drivers / NETBT > Properties > záložka Driver* > zastaviť a zmeniť *Startup Type* zo *System* na *Disabled*.
- SK: *Ovládací panel/Hardvér a zvuk/Správca zariadení, Zobraziť\Zobraziť skryté zariadenia*
- */Sieťové adaptéry, Wan Miniport IPv6* – v záložke *Ovládač* stlačiť *Zakázať*
- */Sieťové adaptéry, Microsoft ISATAP adapter (IPv6 tunnel* – v záložke *Ovládač* stlačiť *Zakázať*
- */Sieťové adaptéry, Teredo Tunneling Pseudo Interface (IPv6 tunnel* – v záložke *Ovládač* stlačiť *Zakázať*
- */Ovládače bez podpory Plug and Play /Remote Access IPv6 ARP Driver > Vlastnosti* > záložka *Ovládač*: Zmeniť typ *Pri spustení* zo *Systém* na *Vypnuté*
- */Non-Plug and Play Drivers / NETBT > Vlastnosti* > záložka *Ovládač*: *Zastaviť* a Zmeniť typ P*ri spustení*" zo *Systém* na *Vypnuté*. Opatrenie neaplikujeme na zariadenia pripojené v doméne. (Vypnutý NETBIOS úplne/čiastočne zatvorí port 445)

Dôvod :

NetBT driver je *NetBIOS*. Závisí od neho služba TCP/IP *NetBIOS Helper*. Ak vypneme *NetBT* driver,

nebude dostupná funkcionalita *NetBIOS*-u. Ak je naše zariadenie samostatne stojace (tzv. standalone), toto je želaný stav.

Pri vypínaní určitej funkcie sa odporúča vypnúť aj jej komponenty. Takže napriek tomu, že sme vyššie znefunkčnili IPv6, mali by sme ešte vypnúť ovládače pre *Wan Miniport IPv6* , *Teredo*, *ISATAP* a *IPv6 ARP driver*.

Možné dôsledky, ak opatrenie neaplikujeme :

Aktívne budú aj nepoužívané, resp. nie nevyhnutné protokoly. Ak službu či protokol nepotrebujeme, vypíname aj ich komponenty. Ak ich necháme aktívne, otvárajú ďalšie možnosti exploitácie ich zraniteľností.

Ako príklad uvedieme problémy spojené s *UPnP*:

Prvým z nich je autentifikácia. Protokol *UPnP* natívne neimplementuje žiadnu autentifikáciu. Preto ju na zariadenia musia inštalovať sami používatelia. Častokrát tak však neurobia a považujú lokálnu sieť a jej používateľov za dôveryhodných.

Ďalším problémom je, že *UPnP* umožňuje voľný prístup z internetu. Zaujímavý prieskum sa uskutočnil v r. 2013, kedy tím počas 6 mesiacov skenoval signály z *UPnP* zariadení, oznamujúcich ich prítomnosť na Internete. Na requesty odpovedalo takmer 7000 zariadení (80% domáce routre, ďalej tlačiarne, webkamery...), z ktorých mnohé boli prístupné a manipulovateľné.

4.3 Vypnúť Link Local Multicast Name Resolution

Stupeň 3

Postup:

1. spustíme *Gpedit.msc* ako správca
2. <SK: *Konfigurácia počítača/*EN: *Computer Configuration>\Administrative Templates \Network\DNS Client\Turn off Multicast Name Resolution* - otvoriť a zmeniť na *Enabled*

Dôvod:

Zmyslom *LLMNR* je získanie IP adresy na základe daného *NetBIOS* mena, bez toho, aby bol prítomný DNS server. Je však výhodné zostať ukrytý, najmä v prípade, že nie sme serverom poskytujúcim služby (napr. webový či súborový server). Navyše sa *LLMNR* snaží posielať pakety na multicastovú adresu 224.0.0.252:5355, tieto pokusy však Firewall blokuje. To znamená, že táto služba bežne nemá význam.

Možné dôsledky, ak opatrenie neaplikujeme :

Naše zariadenie nie je ukryté. Vysielame pakety, ktoré FW blokuje – zbytočné zaťaženie.

4.4 Vypnúť IGMP

Stupeň 3

Postup:

1. Spustiť *Command line (SK: Príkazový riadok)* ako *administrátor*

2. Zadať príkaz Netsh interface ipv4 set global mldlevel=none

Dôvod:

Protokol *IGMP* je v súčasnosti prakticky nepoužívaný, nie je preto dôvod, aby bol aktívny.

Možné dôsledky, ak opatrenie neaplikujeme :

Otvárajú sa možnosti útoku na zraniteľnosti *IGMP* protokolu.

4.5 Vypnúť port 1900 *UPnP*

Stupeň 3, 2, 1

Postup:

1. spustíme *Regedit* ako správca

2. nájsť register *HKEY_LOCAL_MACHINE\Software\Microsoft\DirectplayNATHelp\DPNHUPnP*

3. Pravým tlačidlom kliknúť na pravý panel okna – vytvoríme *new dword:32 bit*, ktoré pomenujeme *UpnPMode*

4. Dvojklikom nové DWORD otvoríme a nastavíme hodnotu na *2* (*value: 2*).

Dôvod:

Cieľom *UPnP* je aj zjednodušenie konfigurácie, napríklad na udelenie výnimky vo firewalle pre hry a podobne. Nový hráč sa na prevádzkujúcu stanicu pripojí, pritom sa automaticky nakonfigurujú FW pravidlá, aby mu bol prístup umožnený. To však má za následok množstvo neprehľadných pravidiel. Preto ho podľa možnosti vypneme a FW pravidlá nakonfigurujeme manuálne.

Možné dôsledky, ak opatrenie neaplikujeme :

Automatické vytváranie FW pravidiel povedie skôr či neskôr k ich neprehľadnosti. Administrátor nemá plnú kontrolu nad stavom a funkčnosťou FW. Ak je nových pravidiel priveľa, FW stráca na účinnosti. Akýkoľvek útok zvonka je uľahčený. Navyše, ak sa napr. útočník za hráča hry iba vydáva, je mu novou výnimkou vo FW umožnený prístup do nášho systému. Pridelené mu budú práva na úrovni používateľa Ak ale nie sú aplikované ďalšie bezpečnostné opatrenia, môže práva eskalovať na privilegovanejších používateľov. *UPnP* vždy predstavuje bezpečnostné riziko, lebo umožňuje automatické pripojenie sa k sieti a prostriedkom na nej.

4.6 Vypnutie všetkých nepotrebných aplikácií, ktoré počúvajú na portoch

Stupeň 3

Postup:

1. Spustiť *Command line* ako administrátor

2. Zistiť, aké aplikácie na portoch počúvajú, príkazom netstat -abn. Počúvať má :

- RPC (Port 135)
- Wininit.exe (49152)
- eventlog (49153)
- schedule service (49154)
- services.exe (49155)
- lsass.exe (49156)

3. Všetky ostatné aplikácie, pokiaľ nie sú potrebné, je možné vypnúť, napr. pomocou cmd:

taskkill /IM [/F] <meno_aplikácie>

Dôvod:

Všetky aplikácie, ktoré nie sú pre beh počítača nevyhnutné, nemajú byť zapnuté a počúvať na portoch sieť. S počúvajúcim procesom možno totiž nadviazať komunikáciu – aj škodlivú. Vyššie uvedené počúvajúce aplikácie sú nevyhnutné pre správny beh Windows 7, ostatné preto môžu byť zastavené.

Možné dôsledky, ak opatrenie neaplikujeme :

Neočakávané počúvajúce aplikácie môžu byť znakom prieniku do systému – napr. spustí sa proces, pomocou ktorého malware komunikuje s útočníkom. Neškodná počúvajúca aplikácia je vystavená riziku nadviazania neželanej, potenciálne škodlivej komunikácie.

4.7 Nastavenie firewallu

Stupeň 3, 2, 1

Postup:

*1. Ovládací panel/Systém a zabezpečenie/Nástroje na správu/Windows Firewall with Advanced Security /*odkaz na pravej lište *"Vlastnosti"*

alternatívne *Local Security Policy/ Konfigurácia počítača / Nastavenie Systému Windows / Security Settings / Windows Firewall with Advanced Security*

2. Rozklikneme každý profil (záložky *Domain, Private, Public*) a nasledovne zmeníme:

- zmeniť *Outbound connection = Block*

- špecifikovať nastavenia správania sa FW: *Settings that control Windows Firewall Behavior > Customize*

-- nastaviť *Allow Unicast Response: No*

- špecifikovať nastavenia logovania:

Specify Logging settings for Troubleshooting > Customize

-- *Size Limit = 32767 KB*

-- *Log Dropped packets = Yes*

3. Definovať nižšie uvedené pravidlá pre prichádzajúce a odchádzajúce spojenia, služby, programy a porty. Pravým tlačidlom klikneme na *Outbound Rules* (resp. *Inbound*) na ľavom paneli a vyberieme *New rule...* V zobrazenom sprievodcovi definujeme pravidlo pre program (*Program*), port (*Port*) alebo zvolíme *Customize*. To nám umožní určiť detailnejšie program, protokol, službu, číslo portov či IP adresy, na ktoré sa pravidlo má aplikovať.

Pre pravidlo ďalej určujeme akciu, vykonanú po nájdení zhody s pravidlom:

- *Allow the connection* – spojenie je povolené
- *Allow the connection if it is secure* – komunikácia bude povolená iba ak je zabezpečená cez IPSec
- *Block the connection* – komunikácia bude blokovaná

Napokon určíme profil, v ktorom sa má pravidlo aplikovať: ak je PC pripojený do domény (*Domain*) a/alebo ak je v súkromnej (*Private*) alebo verejnej sieti (*Public*). Po zadaní mena bude nové pravidlo vytvorené.

Pravidlá : *allow* = povoliť, *disable* = vypnúť, *enable* = zapnúť

In/Out	profil	pravidlo	popis
Outbound	D,Pr,P	**allow service 'Windows Update'**	Povolíme kvôli aktualizácií systému.
Outbound	D,Pr,P	**allow service 'Windows Time'**	Povolíme kvôli synchronizácií času.
Outbound	D,Pr,P	**allow program '\Windows\HelpPane.exe'**	*Windows Help*, umožníme získavanie pomoci z online zdrojov.
Outbound	D,Pr,P	**allow program '\Program Files\Windows Defender\msacui.exe'**	*WinDefender* je skenovací SW na malware, umožníme mu komunikovať s vonkajšou sieťou a aktualizovať sa.
Outbound	D,Pr,P	**allow program <Firefox/ Chrome/ Opera, či iný spustiteľný súbor**	Nevyhnutné, aby prehliadače plnili svoju

		webového prehliadača>	úlohu.
Outbound	D,Pr,P	**allow program \Program Files\Internet Explorer\iexplore.exe**	Povolenie 32 bitovej verzie IE.
Outbound	D,Pr,P	**allow program \Program Files x86\Internet Explorer\iexplore.exe**	Povolenie 64 bitovej verzie IE.
Outbound	D,Pr,P	**allow program <aktualizačný program antimalware riešenia>**	Aktualizácia antimalware riešenia.
Outbound	D,Pr,P	**allow program "%ProgramFiles% (x86\Secunia\PSI\psia.exe"**	*Secunia Personal Software Inspector (PSI)* je free bezpečnostný nástroj na identifikáciu zraniteľností v ne-MS programoch. Scanuje aplikácie, či im nechýbajú bezpečnostné záplaty, a automaticky aktualizuje systém, alebo oznamuje prítomnosť novej aktualizácie
Outbound	D,Pr,P	**allow program "%ProgramFiles% (x86\Secunia\PSI\psi.exe"**	Detto.
Outbound	D,Pr,P	**disable all Core Networking rules that mentions IPv6, Teredo, and ICMPv6**	SK: *Základná prevádzka siete* Znefunkčnenie pravidiel týkajúcich sa IPv6 protokolovej komunikácie. Dôvody vysvetlené vyššie.
Outbound	D,Pr,P	**disable Core Networking IPHTTPS**	Vypnutie *IPHTTPS (*teda tunelovanie IPv6 packetov cez *HTTPS)*.
Outbound	D,Pr,P	**disable Core Networking IGMP-out**	Vypnutie protokolu *IGMP (*podpora pre *IP multicast)*.
Outbound	D,Pr,P	**disable all Core Networking rules that mention Group policy** **SK: Základná prevádzka siete - Skupinová politika**	Pravidlá pre skupinovú politiku budú explicitne definované pre PC pripojený do siete. Platí iba v prípade, že PC nie je zapojené do domény, inak nemá byť táto prevádzka povolená. Nemá zmysel pre PC mimo domény.
Outbound	D,Pr,P	**disable the 2 rules that mentions HomeGroup**	Službu *HomeGroup* sme deaktivovali, viď predošlé sekcie dokumentu.
Outbound	D,Pr,P	**disable all rules for Remote**	Pravidlá týkajúce sa *Pomoci na diaľku* – nie je žiadúce, aby sa ktokoľvek mohol

		Assistance	na náš PC pripájať, hoci za účelom pomoci a cez šifrované spojenie.
Outbound	Pr	**disable all Network Discovery rules for private profile (NB-Datagram-out, NB Name out, LLMNR UDP Out, Pub-WSD-out, SSDP-out, UPnP-Host-Out, UPnP-Out, WSD-Events-Out, WSD-EventsSecure-Out and WSD-Out.**	SK: *Zisťovanie siete*; Všetky odchádzajúce prenosy na zisťovanie siete pre privátny profil zakazujeme; privátny profil indikuje PC v privátnej sieti (domáca alebo pracovná), vypíname preto služby súvisiace s týmito pravidlami, napr. *UPnP* (spomínané na inom mieste dokumentu); ak je zariadenie pripojené do domény, do pravidla nezahrnieme *NB-Datagram-out* a *NB-Name-out*;
Outbound	D,Pr,P	**allow <Adobe Flash Update service>**	Aktualizácia *AdobeFlash*.
Outbound	D,Pr,P	**allow <Adobe Acrobat Update service>**	*Adobe Acrobat* aktualizácia.
Outbound	D,Pr,P	**allow Core Networking DHCP-out**	*DHCP* povolíme kvôli získaniu IP adresy.
Nižšie uvedené vyznačené pravidlá sú nevyhnutné na pripojenie do domény, nastavujeme ich preto v profiloch *Private* a *Domain*			
Outbound	**D,Pr**	**allow LanMan Workstation (v zozname len ako Workstation) service to TCP ports 49152-65535 on Server IP**	Služba *Workstation* vytvára a udržiava klientské sieťové spojenia so vzdialenými servermi pomocou *SMB* protokolu. Je nutná na zdieľanie súborov a tlačiarní na sieti. (*Pri konfigurácií pravidla nastavujeme remote specific ports, remote IP address DNS* servera, teda nášho doménového radiča, na ktorom *DNS* beží)

Outbound	**D,Pr**	**allow \Windows\System32\Lsass.exe to TCP ports 49152-65535 on Server IP**	Povolenie *Local Security Authentication Servera*. Overuje platnosť prihlásení na PC či server. Vytvára proces zodpovedajúci za autentifikáciu používateľov pre službu *WinLogon*.
Outbound	**D,Pr**	**allow Netlogon service to Server IP**	Služba *NetLogon* je podmienkou na pripojenie sa k doménovému radiču. Udržiava zabezpečený kanál na autentifikáciu používateľov a služieb medzi PC a doménovým radičom.
Outbound	**D,Pr**	**allow RPCss service to Server IP**	Služba *Remote Procedure Call* je *Service Control Manager* pre COM a DCOM (*Distributed Component Object Management*) servery. Nevyhnutný pre ich správne fungovanie, ako aj pre funkciu množstva iných procesov.
Outbound	**D,Pr**	**allow to TCP 135 on Server IP**	Detto kvôli *RPC*.
Outbound	**D,Pr**	**allow to TCP 389 on Server IP**	Port pre *Active Diretory*.
Outbound	**D,Pr**	**allow to UDP 389 on Server IP (Active Directory**	Port pre *Active Diretory*.
Outbound	**D,Pr**	**allow to TCP 445 on Server IP**	Port pre *NetBIOS* nad TCP/IP
Outbound	**D,Pr**	**allow to TCP 53 on Server IP**	Port pre *DNS*.
utbound	**D,Pr**	**allow to UDP 53 on Server IP**	Port pre *DNS*.
Outbound	**D,Pr**	**allow to TCP 88 on Server IP**	Port pre protokol *KERBEROS*
Outbound	**D,Pr**	**allow to UDP 88 on Server IP**	Port pre protokol *KERBEROS*
Outbound	**D,Pr**	**allow to UDP 137 on Server IP**	Port pre protokol *NetBIOS*
Outbound	**D,Pr**	**allow to UDP 138 on Server IP**	Port pre protokol *NetBIOS*

Outbound	**D,Pr**	**allow Core Networking Group Policy 3 built-in rules**	Pravidlá pre šírenie skupinovej politiky na doménovej či privátnej sieti; ak nie sme pripojení do domény, vypíname ho.
Outbound	**D,Pr**	**allow Core Networking DNS**	Vstavané pravidlo, ak nie sme pripojení do domény, deaktivujeme ho.
Outbound	**Pr**	**allow Network Discovery NB Datagram Out - Private profile**	
Outbound	**Pr**	**allow Network Discovery NB Name Out - Private profile**	
InBound	**Pr**	**allow Network Discovery NB Datagram In - Private profile**	
InBound	**Pr**	**allow Network Discovery NB Name In - Private profile**	
InBound	D,Pr,P	**allow Core Networking ICMPv4 in**	Povolenie prichádzajúcej *ICMPv4* prevádzky.
InBound	D,Pr,P	**allow Core Networking DHCP in**	Povolenie prichádzajúcich *DHCP* paketov.
InBound	D,Pr,P	**Allow to port 3389**	Port pre *Remote Desktop Protocol(RDP)*
InBound	D,Pr,P	**disable Core Networking IPHTTPS in**	Zakázanie *HTTPS* zabezpečenej komunikácie prichádzajúcej zvonka.
InBound	D,Pr,P	**disable Core Networking IGMP in**	Zakázanie nepoužívaného *IGMP* protokolu, vysvetlené vyššie.
InBound	D,Pr,P	**disable all Core Networking rules that mention IPv6, Teredo, and ICMPv6**	Zakázanie všetkých IPv6 súčastí, vysvetlené vyššie.
InBound	D,Pr,P	**disable the 2 rules that mention HomeGroup**	Nechceme povoliť komunikáciu cez *Home Group*, vysvetlené vyššie.
InBound	Pr	**disable all Network Discovery rules for private profile (NB Datagram in, NB Name in, LLMNR UDP In, Pub-**	Zakazujeme z rovnakých dôvodov, ako obdobné Outbound pravidlo. Opäť, ak je zariadenie pripojené do domény, do

		WSD-In, SSDP-In, UPnP-In, WSD-Events-In, WSD-EventsSecure-In, WSD-In	pravidla nezahrnieme *NB-Datagram-in* ani *NB-Name-in*;	
InBound	D,Pr,P	**disable all rules for Remote Assistance**	*SK: Pomoc na diaľku.* Je nežiadúce, aby na bežnú stanicu bol možný prístup cez *Remote Assistance,* preto zakazujeme.	

Dôvod:

Defaultná politika Windows FW je odmietať akúkoľvek prichádzajúcu komunikáciu (*Inbound: Deny all)* a povoliť všetku odchádzajúcu prevádzku (*Outbound: Allow all)*. Znamená to, že ak je na našej stanici malware, defaultne mu je umožnené komunikovať s jeho riadiacim severom. Zapneme preto blokovanie odchádzajúcej prevádzky a povolíme len tie programy a služby, ktoré potrebujeme a ktoré pre svoju funkciu nevyhnutne prístup na sieť potrebujú. Pri inštalácií nových programov, napr. antivírusového produktu alebo *Microsoft Security Compliance Managera* (budú ešte spomenuté), je potrebné overiť, či nie sú firewallom blokované. Ak by boli, antivírusová databáza by sa neaktualizovala, bezpečnostné šablóny takisto, čím by bol systém zraniteľný a programy inštalované zbytočne.

5 Inštalácia softvéru

5.1 Inštalácia FIXIT

Stupeň 3

Postup - Vypnutie *IPv6* :

1. Zo stránky http://support.microsoft.com/kb/929852 spustíme utilitu *FixIt* – buď na kompletné znefunkčnenie IPv6 (*Disable IPv6 (entirely)*), alebo jeho odstránenie z tunelovacích rozhraní *(Disable IPv6 tunnel interfaces)*.

2. Postup - Vypnutie *AutoRun* :
Zo stránky http://support.microsoft.com/kb/967715 stiahneme a spustíme utilitu *FixIt.*

Dôvod:

Ako sme spomínali vyššie: prechod na *IPv6* protokol je pozvoľný a väčšina sieťových prvkov a služieb vyžaduje na svoju funkciu iba *IPv4* protokol. Preto *IPv6* a jeho súčasti vypíname.

AutoRun je technológia používaná na spustenie programov či rozšíreného obsahu (napr. video na hudobnom CD) automaticky po vložení média do počítača. V tom sa odlišuje od vyššie spomínaného *AutoPlay*, hoci výsledok býva častokrát rovnaký: po vložení média sa tento automaticky spustí, použijúc určitý program. Po vložení média sa spustí *AutoPlay* s otázkou, akú akciu chceme s médiom vykonať. Jednou z možností býva práve spustenie *AutoRun*. V princípe teda nemožno spustiť *AutoRun* bez *AutoPlay*. *AutoRun* je súčasťou typov médií ktoré ho používajú a nedá sa modifikovať. Sú s ním spojené rovnaké riziká ako s *AutoPlay*, preto ho pomocou *FixIt* vypíname.

Možné dôsledky, ak opatrenie neaplikujeme :

Každý aktívne nepoužívaný protokol, ktorý na zariadení necháme spustený, otvára ďalšie možnosti exploitácie jeho zraniteľností.

V prípade *AutoRun* sa vystavuje systém rizikám ako pri *AutoPlay*.

5.2 Inštalácia a konfigurácia antimalware riešenia

Stupeň 3

Dôvod:

Antimalware riešenie je potrebné pre detekciu a odstránenie známeho škodlivého kódu. Mnohé antimalware riešenie ponúkajú aj host based IPS.

Zdarma je možné používať napríklad riešenia :

- AVG
- Windows Security essentials

- AVAST

Platené verzie :

- Microsoft Forefront Security
- Eset Smart Security
- Symantec Endpoint Protection

Antimalware riešenie je potrebné nakonfigurovať na pravidelnú kontrolu a inštaláciu aktualizácií (ideálne každú hodinu) a pravidelnú kontrolu pamäte s súborového systému. Rovnako je preň potrebné nakonfigurovať pravidlo vo firewalle na aktualizáciu antimalware riešenia.

5.3 Inštalácia Security Compliance šablón

Stupeň 3

Postup:

1. Zo stránky stiahneme a nainštalujeme *Microsoft Security Compliance Manager* (viď Referencie). Manager slúži na automatické sťahovanie a aktualizáciu šablón. Na ochranu PC potrebujeme nasledovné:

- Win7SP1 Computer Security Compliance
- Win7SP1 Domain Security Compliance
- Win7SP1 User Security Compliance

2. Na zistenie výsledného setu politík spustíme v Command Line príkaz gpresult /H x.html (spúšťame ako admin, v jeho priečinku sa vytvorí súbor x.html s výsledkami)

3. Pri spustení SCM je na ľavom paneli zoznam šablón pre rôzne platformy. Odporúčaný postup pri zmene konfigurácie je nasledovný:

- vybrať *customize this setting by duplicating baseline*. Vytvorí sa kópia šablóny, ktorú na ľavom paneli vidno pod *Custom Baselines*. Kópiu editujeme podľa svojich potrieb.

4. Šablóny možno importovať nasledovne:

A. Importujeme sadu politík nastavených v Active Directory našej domény (na pravej strane okna vyberieme *Import – SCM(.cab)*).

B. Importujeme konfiguráciu referenčného PC, na ktorom sme urobili všetky potrebné zmeny nastavení. Získame ju pomocou *LocalGPO* nástroja vytvorením zálohy lokálnej skupinovej politiky, ktorú následne importujeme.

Zálohu získame vybraním *Export GPO Backup* na pravom paneli. Zvolíme priečinok, do ktorého sa vytvorí adresár so zašifrovaným menom. V ňom budú aktuálne nastavenia, uložené vo viacerých súboroch.

Nainštalujeme *LocalGPO* nástroj (nástroj príkazového riadku na inštaláciu a aktiváciu *GPO Backup*, súčasť *SCM*, inštalátor možno nájsť v priečinku *C:\Program Files (x86)\Microsoft Security Compliance Manager\LGPO*).

- Aktivácia backup šablóny: V priečinku *C:\Program Files (x86)* vyberieme *LocalGPO,* klikneme pravým na *Command Line Here.cmd* a spustíme ako správca. Zadáme
- *cscript LocalGPO.wsf /Path:<cesta k adresáru s vytvorenou zálohou>*
- Tým sme šablónu zo zálohy preniesli a aktivovali.
- Návrat pôvodných nastavení: príkaz *LocalGPO*
- *cscript LocalGPO.wsf /Restore*
- Upozornenie: aby import lokálnej politiky prebehol správne, musíme expotrovať a prenášať aj *Win7SP1 Domain Security Compliance.* Táto šablóna upravuje politiku tvorby hesiel a uzamknutia konta používateľa (vysvetlené nižšie), od nich závisia aj používateľské politiky.

Poznámky

- Inštalácia vyžaduje prítomnosť .NET Framework, Visual Studio a SQL(Ak SQL server nie je prítomný, Sprievodca inštaláciou nás vyzve, či ho chceme inštalovať teraz; Visual Studio sa stiahne súčasne s .NET.)
- Musíme pridať firewallové pravidlo, aby neboli MSC aktualizácie blokované: *Outbound* rule pre profily *Private, Public, Domain* a pre program *C:\Program Files (x86\Microsoft Security Compliance Manager\ Microsoft Security Compliance Manager.exe*

Dôvod:

Security Compliance šablóny umožňujú rýchle zosilnenie Windows systémov. Jednoducho stiahneme baseline security template, určený pre náš systém, a nastavíme želanú konfiguráciu. Nástroj MSC slúži na automatické sťahovanie, aktualizáciu a prehľadnú konfiguráciu bezpečnostných nastavení systému. Nastavenia sa týkajú lokálnych bezpečnostných politík (*Local Security Policies*) a skupinových politík (*Group Policies*). Poskytuje vysvetlenie všetkých nastavení, sumarizuje zraniteľnosti a opatrenia na ich zmiernenie. Nastavenia možno aplikovať tak na samostatné PC, ako aj na celú doménu. Bezpečnostné politiky je možné nastavovať na jednotlivých zariadeniach osobitne, pomocou MSC však stačí konfigurovať jediné zariadenie a príslušné politiky preniesť na ostatné stanice.

Všímame si najmä politiky z okruhov *Computer, Domain* a *User Security Compliance*. Každá s nich obsahuje pravidlá, rozdelené do skupín podľa vzájomnej súvislosti:

Computer – Authentication Types (Typy autentifikácie), *Encryption Configuration* (Konfigurácia šifrovania), *Event Logging* (Zaznamenávanie udalostí), *File System* (Súborový systém), *Identity Management* (Manažment identity), *Key Management* (Manažment kľúčov), *Least Functionality*

(Princíp najmenšej funkcionality), *Least Privilege* (Princíp najnižších privilégií), *Log Access Limitation* (Obmedzenie prístupu k logom), *Logging Configuration* (Nastavenie logovania), *Network Protection* (Ochrana siete), *Password Attributes* (Vlastnosti hesla), *Protocol Configuration* (Nastavenie protokolov), *Remote Access* (Vzdialený prístup), *Session Configuration* (Konfigurácia relácií), *System Defaults* (Východiskové nastavenia systému), *System Integrity* (Integrita systému), *User Notification*(Notifikácia používateľa). Z pravidiel sú zaujímavé napríklad nasledovné:

- *Remote Access*: *Allow log on through Remote Desktop Services, Allow users to connect remotely using Remote Desktop Services, Allow Remote Shell Access, Deny log on through Remote Desktop Services* upravujú prístup k PC, resp. pripojenie na iné PC, pomocou *RDS* a vytvorenie *Remote Shell* prístupu;

- *Key Management*: *Domain member: Requite strong(Windows 2000 or later) session* – vyžaduje použitie silného (min. 128-bitového) kľúča na vytvorenie zabezpečeného spojenia s doménovým radičom;

- *Least Functionality*: *Interactive logon: Do not require CTRL+ALT+DEL* – ak túto politiku povolíme, používatelia sa môžu prihlasovať bez zadania uvedenej kombinácie kláves; *Turn off AutoPlay* – zakázanie alebo povolenie automatického prehrávania z médií pripojených k PC;

- *Password Attributes*: pravidlá upravujú, či používateľ musí zadať heslo po návrate PC z režimu spánku, kedy je upozornený na blížiace sa vypršanie hesla, či môže byť konto s prázdnym heslom použité na prihlásenie z iného ako lokálneho systému a pod.

- *Network Security: LAN Manager authentication level:* Umožňuje vyžadovať najnovšiu verziu autentifikácie – NTLMv2. Zakážeme tak staršiu LM aj NTLM autentifikáciu. Toto je mimoriadne dôležité pravidlo, nakoľko autentifikácia slúži na zaradenie stroja do domény a definovaný protokol sa používa i na autentifikáciu medzi doménami či medzi doménovými radičmi. Je preto nutné použiť silný algoritmus.

- *Encryption Configuration:* o.i. je dôležité napríklad správne nastavenie SMB podpisovania a šifrovania: *Microsoft network client: Digitally sign communications(always), Microsoft network client: Digitally sign communications(if server agrees)* – tieto pravidlá nastavíme na Enabled, čím vynútime SBM podpisovanie na strane klienta; konfiguráciou politiky *Microsoft network client: Send unencrypted password to third-party SMB servers* zabránime posielaniu *SBM* hesla v otvorenej forme. Všimnime si, že uvedené nastavenia sa týkajú strany klienta, obdobné nastavenia existujú a majú byť nakonfigurované aj na strane servera.

  <u>*Domain*</u> – 2 skupiny pravidiel, ktoré popíšeme podrobnejšie:

- *Account Lock* (Uzamknutie konta)

- pravidlo *Account lockout threshold*: maximálny dovolený počet neplatných prihlásení, kým sa konto neuzamkne;

- *Reset account lockout counter after*: Určuje dobu, po ktorej uplynutí sa počítadlo neplatných prihlásení resetuje na 0;

- *Account lockout duration*: Určuje dobu, počas ktorej je konto uzamknuté;

- *Password Attributes* (Vlastnosti hesla)

  - *Minimum password length*: stanovuje miknimálny počet znakov používateľovho hesla

  - *Minimum password age*: definuje najmenší počet dní, ktorý musí byť heslo v platnosti, kým si ho používateľ môže zmeniť; spolu s *Enforce PSW history* predchádza znovupoužívaniu hesiel (malo by byť nastavené na viac ako 1 deň)

  - *Password must meet complexity requirements*: požiadavky na zložitosť hesla:

    - nesmie obsahovať prihlasovacie meno ani časť jeho skutočného mena dlhšiu ako 2 znaky,
    - dĺžka je min. 6 znakov,
    - obsahuje 3 druhy znakov spomedzi 4 skupín (anglické veľké a malé písmená: A-Z a a-z, základné číslice 0-9, nealfabetické znaky ako !,€,#,%) ; piata kategória sú regionálne špecifické Unicode znaky, tie sem nezaraďujeme;

  - *Maximum password age*: maximálna doba platnosti hesla, musí byť menej ako 90 dní;

  - *Store passwords using reversible encryption*: Určuje, či OS môže ukladať heslá v reverzibilne zašifrovanej podobe, aby ich mohli využívať aplikácie na autentifikáciu používateľa; tento formát je omnoho slabší, ukladané heslá sú omnoho ľahšie kompromitovateľné, preto by ukladanie nemalo byť povolené;

  - *Enforce password history* – určuje počet nových, unikátnych hesiel, ktoré musia byť previazané s konkrétnym používateľom, kým mu je umožnené heslo opätovne použiť; minimálna hodnota pre doménového používateľa je 24.

<u>User</u> – pravidlá zoskupené do tém *Administrative Templates**System for user setting, Control Panel**Display for user setting, Windows Components**Attachment Manager for User Setting, Windows Components**Windows Explorer for User Setting*

<u>Možné dôsledky, ak opatrenie neaplikujeme</u>:

Bezpečnostné opatrenia navrhované firmou Microsoft sú adresované na pokrytie štandardných bezpečnostných hrozieb a ošetrenie základných bezpečnostných problémov pri používaní systému Windows. Tieto opatrenia nie sú nastavené ako defaultné z dôvodu zníženia komfortu využitia pracovnej stanie s operačným systémom Windows.

Pri postupnom zabezpečovaní systému manuálne môže dôjsť ku chybe či vynechaniu niektorých krokov. Najmä pri zložitejšej konfigurácií je časová úspora cenná. Výhodná je možnosť aplikácie opatrení na celú doménu. Okrem rýchlosti zabezpečí, že každý systém v doméne má jednotné bezpečnostné nastavenie. Každé pravidlo v baseline obsahuje popis zraniteľnosti, proti ktorej bojuje. Ignorovaním pravidla sa uvedeným zraniteľnostiam vystavujeme.

5.4 Inštalácia a spustenie EMET

Stupeň 3

Postup:

1. Zo stránky produktu (viď Referencie) si nástroj EMET stiahneme a spustíme inštaláciu.
2. Spustíme EMET a otvoríme možnosť konfigurácie (ak nie je otvorená priamo v GUI) - Configure System, a vykonáme nasledovné nastavenia:
   - DEP - always on
   - SEHOP - always on
   - ASLR - application opt in
   - Pinning: Enabled
3. Stlačíme *Apps*, potom *Add Application*. Najdeme a pridáme nasledovné aplikácie:
   - \Windows\System32\wuauclt.exe
   - \Windows\servicing\trustedinstaller.exe
   - inštalovaný antivírus
   - všetky aplikácie, ktoré pre svoju funkciu potrebujú komunikovať cez Internet (t.j. ktoré majú za vstup stiahnuté dáta): prehliadače, media player, Adobe Reader... (pridali sme IE, Mozilla, MS Security Compliance Manager)

Dôvod:

Microsoft EMET je nástroj na implementáciu techník zabraňujúcich útočníkom exploitáciu zranitelností v systéme Windows a inštalovaných aplikáciach.

Implementované techniky zahŕňajú:

- SEHOP - Structured Exception Handler Overwrite Protection:

Ochrana pred najčastejším spôsobom exploitácie zraniteľností typu *Stack Overflow* – pretečenie zásobníka - na Windowsoch. Možno ju aktivovať na per-process báze. Bez EMETu môže útočník prepísať riadenou hodnotou handler pointer na záznam o výnimkách na stacku. Keď nastane výnimka, operačný systém prechádza reťaz záznamov o výnimkách. Keďže útočník jeden z nich kontroluje, OS preskočí na lubovoľné iné miesto, kam ho útočník nasmeruje s tým, že mu tak odovzdá riadenie nad behom vykonávania. EMET zabezpečí, že predtým, ako OS zavolá obsluhu výnimky, overí si reťaz záznamov o výnimkách. Overenie zahŕňa kontrolu, či finálna výnimka obsahuje aj preddefinovanú. Ak

bola reťaz porušená,, EMET proces ukončí bez volania handlerov výnimiek.

- DEP – Data Execution Prevention

Bez EMETu sa útočník môže pokúsiť exploitovať zraniteľnosť skokom do shellkódu na takom mieste v pamäti, kde sa nachádzajú útočníkom riadené dáta (napr. na zásobníku či halde). Tieto lokality sú označené ako vykonávateľné, preto bude škodlivému kódu umožnené zbehnúť. Zapnutím EMETu je pre daný proces aktivovaný DEP. Tým sa stack aj heap označí ako nevykonateľný a akýkoľvek pokus o vykonanie škodlivého kódu z týchto lokalít bude odmietnuté na úrovni procesora. Aplikácie môžu byť zvolené na individuálnej báze, ak aj neboli skompilované so špeciálnym flagom. V minulosti to možné nebolo.

- HeapSpray Allocation

Keď expolit beží, častokrát nie je isté, kde presne sa jeho kód nachádza. Preto pri preberaní riadenia instruction pointera „háda“. Aby zvýšili šance na správny tip, väčšina *dnešných* exploitov používa tzv. heapspray techniky, kedy umiestňujú kópie svojho kódu na čo najväčší počet pamäťových miest. EMET prealokuje určité často používané stránky pamäte, takže na ne kód nemôže byť umiestnený, exploit sa nemôže spoliehať na to, že ich riadi a preskočiť na ne.

- NullPage Allocation

Ide o podobnú techniku, ako HeapSpray alokácia, navrhnutá však na prevenciu výskytov potenciálnych nulových dereferencií (dereferencujeme premennú, ktorá nebola inicializovaná, t.j. pýtame sa na hodnotu, ktorá je uložená „nikde“) v používateľskom móde. V *súčasnosti* nie sú známe možnosti ich exploitácie, ide teda o hĺbkovú ochranu.

- Mandatory ASLR – Adress Space Layout Randomization

ASLR znáhodňuje adresy, na ktoré sú načítavané moduly. Tak predchádza tomu, aby útočník vytipoval umiestnenie dát na predikovateľných adresách. Problémom je, že na to, aby boli zapojené, musia všetky moduly používať *compile time* flag. Bez EMETu môže útočník využiť predpovedateľné mapovanie dll a použiť ich na obídenie DEP pomocou techniky ROP (Return Oriented Programming). EMET vynúti načítanie všetkých modulov cieľového procesu na znáhodnené adresy, bez ohľadu na flag, s akým boli kompilované. Exploity používajúce ROP a spoliehajúce sa na predpovedateľné mapovanie zlyhajú.

- Export Address Table Access Filtering

Na vykonanie „zmysluplnej“ akcie potrebuje shellkód zavolať Windows API. Na to však musí zistiť, na akej adrese je API načítané. Na to väčšina shellskriptov prechádza tabuľkou všetkých načítaných modulov, aby našli moduly obsahujúce užitočné API. Obvykle to zahŕňa kernel32.dll a ntdll.dll. Po nájdení modulu už skript vie odhadnúť, kde v ňom sa nachádza API. EMET filtruje prístupy do EAT - Export Address Table, pričom povoľuje a odmieta prístup na čítanie/zápis na základe volacieho kódu procesu. Väčšina *dnešných* exploitov tak je zablokovaná. Opatrenie sa bije s niektorými programami, napr. debbugermi či SW, ktoré sa tak správajú alebo používajú antidebuggovacie techniky (ochranné mechanizmy, DRB, unpackery).

- Bottom-Up randomization

Táto technika mitigácie znáhodňuje bázovú adresu bottom-up alokácie (haldy, stacky, iné lokality pamäti) 8 bitmi entropie. Znáhodnenie funguje okamžite po jeho povolení v EMETe, nepôsobí spätne

na predtým alokované miesta.

- ROP Mitigations

ROP je technikou exploitácie, ktorá umožňuje vykonanie kódu aj v prítomnosti opatrení ako DEP. ROP používa úryvky kódu, ktoré sa už v aplikácií nachádzajú. ROP opatrenia fungujú asi takto:

1. Kontrola načítavania knižníc – EMET monitoruje volania LoadLibrary API a bráni načítaniu knižníc z UNC ciest. Toto sa dá vypnúť pre prípad, že náš program oprávnene načítava DLLky z UNC ciest či vzdialených serverov.
2. Kontrola ochrany pamäte – EMET zakáže označenie stacku za vykonateľný. Takáto akcia je obvykle použitá shellmi a ROP nástrojmi.
3. Kontrola volaní – EMET sa uistí, že keď je dosiahnutá kritická funkcia, je dosiahnutá cez inštrukciu volania, nie cez RET. Toto opatrenie je veľmi účinné a zlomí mnohé ROP nástroje. Môže byť nekompatibilné s niektorými programami.
4. Simulácia toku vykonávania - Snaha o detekciu ROP trikov nasledujúcich volanie kritickej funkcie. Opatrenie môže byť nekompatibilné s niektorými programami.
5. Stack pivot – Opatrenie na detekciu toho, či bol zásobník pivotovaný. S väčšinou programov je kompatibilné.

- Cert trust – configure certificate pinning

EMET poskytuje mechanizmus na dodatočnú kontrolu počas procesu validácie dôveryhodnosti reťaze certifikátu. Cieľom je odhalenie MITM útoku (man-in-the-middle, muž v strede) na šifrovanom kanáli. Zakaždým keď Internet Explorer počas prehliadanie HTTPS stránky vytvorí reťaz pre SSL certifikát, EMET validuje SSL certifikát koncovej entity a koreňovú certifikačnú autoritu (*Root CA*), ktorá cert vydala, oproti zodpovedajúcemu pinning pravidlu, ktoré nakonfiguroval používateľ. Na základe nakonfigurovaných pravidiel pre špecifickú doménu EMET deteguje rozdiel v koreňovej CA pre daný SSL cert. EMET však nepreruší spojenie. EMET páruje *certificate subject name (CN)* SSL certu (vrátane alternatívnych mien) s menom webstránky nakonfigurovanom v pravidlách. Ak je nájdená zhoda, EMET overí že vydávajúca koreňová CA certifikátu je jednou z koreňových CA zvolených používateľom. Sada dôveryhodných koreňových CAsa dá definovať importom ich certov z Windows Trusted Root Certification Authorities store. Po tom môžu byť vytvorené pravidlá asociujúce subjekty SSL certu so špecifickou sadou certifikátov koreňových CA.

Možné dôsledky, ak opatrenie neaplikujeme:

Ako sme uviedli pri popise funkcií EMETu, do značnej miery chráni systém pred nasledovnými typmi exploitov, útokov, zraniteľností:

- Stack Overflow, ROP, MITM
- spustenie škodlivého kódu zo stacku či haldy
- umiestnenie škodlivého kódu na mnohé pamäťové lokácie
- zneužitie faktu, že moduly sú načítané na predikovateľné stránky pamäte
- vyhľadanie modulov so zneužiteľnými API v Export Address Table

6 Inštalácia a konfigurácia internetového prehliadača

Stupeň 3

Postup:

1. Inštalujeme voľne dostupný internetový prehliadač Mozilla Firefox. Nastavíme automatické aktualizácie. Inštalujeme a nakonfigurujeme nasledovné doplnky (záložka *Add-Ons*):

- *Adblock Plus*
  - Blokovať známy malware: *Malware Blocking* nastaviť na ON
  - Zakázať sledovanie: *Disable Tracking* nastaviť na ON
- *NoScript (NoScript Security Suite 2.6.8.40)*
- *Ghostery*
  - Blokovanie všetkých trackerov (nastaviť *Blocking ALL trackers, Save*)

2. Konfigurácia prehliadača:

- Spresnenie (*Firefox Preferences* alebo *Options* > *Advanced* > *Data Choices*)
  - Voľby týkajúce sa Odosielania údajov - odškrtnúť všetky
- Všeobecne (*Firefox Preferences* alebo *Options* > *General*)
  - Označiť voľbu *Vždy sa opýtať, kam súbory uložiť (Always ask me where to save files)*
- Bezpečnosť (*Firefox Preferences* alebo *Options* > *Security*)
  - Odškrtnúť voľbu *Pamätať si heslá stránok (Remember passwords for sites)*

Dôvody a riziká plynúce z ponechania defaultných nastavení:

Blokovanie známeho malware priamo v prehliadači či zákaz spúšťania skriptov sú vhodné mechanizmy na zvýšenie bezpečnosti systému. Zakázaním sledovania obmedzíme množstvo verejne dostupných dát o našom PC a aktivitách na Internete.

Takisto nie je žiadúce, aby boli odosielané akékoľvek údaje o prehliadači, histórií navštívených stránok či systéme. Môžu byť zbierané za účelom neskoršieho zneužitia, napr. podvrhnutie falošnej stránky, maskovanej ako nami preferovaný internetový obchod či phishingový mail od našej banky.

Ukladanie prístupových hesiel v prehliadači je mimoriadne rizikové. Funkcia *"Remember me"* môže byť implementovaná chybne, napr. heslá sa ukladajú v nezašifrovanej forme. Obvyklé je aj ukladanie do perzistentných cookies s loginom alebo s identifikátorom spojenia. Takéto cookies sú v prípade, že ich útočník odchytí, zneužiteľné na krádež účtu.

Napokon ukladanie súborov do predvoleného priečinka môže viesť k nechcenému a nepozorovanému automatickému sťahovaniu škodlivého obsahu. Ak sa pri každom sťahovaní súboru ukáže prompt, používateľ si všimne každý ukladaný súbor. Všimne si pokusy o automatické stiahnutie neželaného obsahu a vie mu zabrániť.

7 Šifrovanie dát

Postup:

BitLocker je súčasť *Windows* 7 verzií *Ultimate* a *Enterprise*, umožňujúca *Full Disk Encryption*. Ak je *BitLocker* aktívny, celý disk bude zašifrovaný a nečitateľné pre iné kópie systému Windows či Linux. Tak sa zamedzí offline útokom na dáta. *BitLocker* je najlepšie použiť na počítači s TMP čipom. Ak však naše zariadenia túto vlastnosť nemajú, možno *BitLocker* nakonfigurovať, aby ukladal dešifrovací kľúč na USB kľúč. Netreba však potom zabúdať na ochranu tohto média.

Dôvod:

Šifrovanie diskov, určitých partícií alebo vybraných súborov by malo byť bežnou praxou najmä pri manipulácií s citlivými údajmi. Existuje množstvo nástrojov, umožňujúcich *Full Disk Encryption* či zašifrovanie obsahu prenosných médií. Rovnako je možné vytvárať šifrované či skryté partície na diskoch. Šifrovacie prostriedky sú tak softvérové, ako aj hardvérové.

Cieľom je zabezpečenie dôvernosti dát, a to aj v prípade, že by bolo odcudzené pamäťové médium či notebook s citlivými informáciami. Ide o pasívnu ochranu v čase, keď je OS mimo prevádzky.

Referencie

http://hardenwindows7forsecurity.com/Harden%20Windows%207%20Home%20Premium%2064bit%20-%20Standalone.html

SRP, AppLocker:

- http://technet.microsoft.com/en-us/library/ee449491%28v=ws.10%29.aspx

Windows Services:

- http://www.blackviper.com/service-configurations/black-vipers-windows-7-service-pack-1-service-configurations/
- http://www.7tutorials.com/which-windows-services-are-safe-disable-when
- https://blog.netnerds.net/2009/10/windows-7-disable-unnecessary-services-on-a-domain-workstation/

MS Security Compliance Manager:

- http://technet.microsoft.com/en-us/library/cc677002.aspx
- http://scap.nist.gov/events/2011/itsac/presentations/day2/Pigin%20-%20Security%20Compliance%20Manager%20%28SCM%29%20v2.pdf

EMET:

- http://technet.microsoft.com/en-us/security/jj653751
- http://www.microsoft.com/en-us/download/details.aspx?id=41138&751be11f-ede8-5a0c-058c-2ee190a24fa6=True
- nová verzia 5.0: http://www.microsoft.com/en-us/download/details.aspx?id=43714