Standard antivirové ochrany

Verze 1.11

**Změny:**

|  |  |  |  |
| --- | --- | --- | --- |
| Datum vydání | Verze | Změna proti předchozí verzi | Změnil (jméno) |
| 21.6.2006 | 0.80 | První draft | Libor Šmíd |
| 14.7.2005 | 1.00 | Finální verze | Stanislav Chýlek |
| 10.8.2006 | 1.10 | Doplněna úprava pro servery v aplikační vrstvě | Libor Šmíd |
| 02.12.2015 | 1.11 | Úprava po nasazení nového antivirového systému | Petr Potůček  Jan Boháč |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Obsah

1. Úvod 3

2. rozsah působnosti Standardu 3

3. Antivirová ochrana elektronické pošty 3

4. Antivirová ochrana souborového systému 5

5. Distribuce antivirových definic 7

6. Antivirová ochrana VIRTUÁLNÍCH SERVERŮ 7

7. Odpovědnost jednotlivých činností 8

8. Schvalovací doložka a platnost standarDu 9

# Úvod

Cílem dokumentu je specifikovat standard antivirové ochrany a definice parametrů antivirové ochrany v ČSSZ.

Standardizována Antivirová ochrana (AVO) je realizována v několika úrovních.

* Antivirová ochrana elektronické pošty
  + Antivirová ochrana na serverech av-gate
  + Antivirová ochrana na pracovních stanicích
* Antivirová ochrana souborového systému
  + Antivirová ochrana na serverech
  + Antivirová ochrana na pracovních stanicích

**Tento dokument patří mezi schválené standardy ČSSZ a je pro zhotovitele závazný.**

# rozsah působnosti Standardu

Tento standard se vztahuje na všechny servery a pracovní stanice v prostředí ČSSZ.

# Antivirová ochrana elektronické pošty

Antivirová ochrana elektronické pošty je zajištována na av-gate serverech produktem InterScan Messaging Security Suite, na cílových exchange serverech antivirus implementován není. Současně je zde i modul pro antispamovou kontrolu.

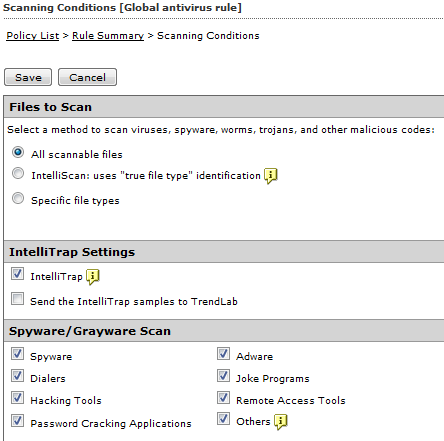
Tabulka zakázaných příloh, které jsou nastaveny na av-gate serverech a uvedena níže, je referenční a koresponduje s nastavením klienta MS Outlook 2003, na systémech Windows 7 SP1 pracovních stanic uživatelů.

|  |  |
| --- | --- |
| **Přípona** | **Popis souboru** |
| **.ade** | Access Project Extension (Microsoft) |
| **.adp** | Access Project (Microsoft) |
| **.app** | Executable Application |
| **.asp** | Active Server Page |
| **.bas** | BASIC Source Code |
| **.bat** | Batch Processing |
| **.cer** | Internet Security Certificate File |
| **.chm** | Compiled HTML Help |
| **.cmd** | DOS CP/M Command File, Command File for Windows NT |
| **.com** | Command |
| **.cpl** | Windows Control Panel Extension (Microsoft) |
| **.crt** | Certificate File |
| **.csh** | csh Script |
| **.exe** | Executable File |
| **.fxp** | FoxPro Compiled Source (Microsoft) |
| **.hlp** | Windows Help File |
| **.hta** | Hypertext Application |
| **.inf** | Information or Setup File |
| **.ins** | IIS Internet Communications Settings (Microsoft) |
| **.isp** | IIS Internet Service Provider Settings (Microsoft) |
| **.its** | Internet Document Set, Internation Translation |
| **.js** | JavaScript Source Code |
| **.jse** | JScript Encoded Script File |
| **.ksh** | UNIX Shell Script |
| **.lnk** | Windows Shortcut File |
| **.mad** | Access Module Shortcut (Microsoft) |
| **.maf** | Access (Microsoft) |
| **.mag** | Access Diagram Shortcut (Microsoft) |
| **.mam** | Access Macro Shortcut (Microsoft) |
| **.maq** | Access Query Shortcut (Microsoft) |
| **.mar** | Access Report Shortcut (Microsoft) |
| **.mas** | Access Stored Procedures (Microsoft) |
| **.mat** | Access Table Shortcut (Microsoft) |
| **.mau** | Media Attachment Unit |
| **.mav** | Access View Shortcut (Microsoft) |
| **.maw** | Access Data Access Page (Microsoft) |
| **.mda** | Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft) |
| **.mdb** | Access Application (Microsoft), MDB Access Database (Microsoft) |
| **.mde** | Access MDE Database File (Microsoft) |
| **.mdt** | Access Add-in Data (Microsoft) |
| **.mdw** | Access Workgroup Information (Microsoft) |
| **.mdz** | Access Wizard Template (Microsoft) |
| **.msc** | Microsoft Management Console Snap-in Control File (Microsoft) |
| **.msi** | Windows Installer File (Microsoft) |
| **.msp** | Windows Installer Patch |
| **.mst** | Windows SDK Setup Transform Script |
| **.ops** | Office Profile Settings File |
| **.pcd** | Visual Test (Microsoft) |
| **.pif** | Windows Program Information File (Microsoft) |
| **.prf** | Windows System File |
| **.prg** | Program File |
| **.pst** | MS Exchange Address Book File, Outlook Personal Folder File (Microsoft) |
| **.reg** | Registration Information/Key for W95/98, Registry Data File |
| **.scf** | Windows Explorer Command |
| **.scr** | Windows Screen Saver |
| **.sct** | Windows Script Component, Foxpro Screen (Microsoft) |
| **.shb** | Windows Shortcut into a Document |
| **.shs** | Shell Scrap Object File |
| **.tmp** | Temporary File/Folder |
| **.url** | Internet Location |
| **.vb** | VBScript File or Any VisualBasic Source |
| **.vbe** | VBScript Encoded Script File |
| **.vbs** | VBScript Script File, Visual Basic for Applications Script |
| **.vsmacros** | Visual Studio .NET Binary-based Macro Project (Microsoft) |
| **.vss** | Visio Stencil (Microsoft) |
| **.vst** | Visio Template (Microsoft) |
| **.vsw** | Visio Workspace File (Microsoft) |
| **.ws** | Windows Script File |
| **.wsc** | Windows Script Component |
| **.wsf** | Windows Script File |

Kontrola elektronické pošty na úrovni pracovní stanice je spuštěna pluginem Microsoft Outlook AutoProtect. Pokud má klient konfigurován outlook pro příjem POP3/IMAP a odchozí poštu SMTP, je používána komponenta Internet Email AutoProtect

Všechny zavirované elektronické zprávy jsou mazány, bez upozornění odesilateli i příjemci, mj. s ohledem na fakt, že při virových epidemiích by notifikace vyvolaly, tzv. nekonečný zpětný efekt, tato politika je nastavena s ohledem na objem přenášených dat elektronické pošty v rámci organizace.

Nastavení na IMMS trendmicro je následující:



Z důvodu ochrany kapacit linek a úložišť bylo nastaveno i omezení pro multimediální přílohy - Pokud e-mail obsahuje MP3, MPEG a AVI větší než 5MB, zpráva jde do karantény.

# Antivirová ochrana souborového systému

Antivirová ochrana souborového systému je realizována klientem Symantec Antivirus Endpoint Protection 12.1.5 (SEP). Na každé vzdálené lokalitě má jeden SEP klient na serveru SIzz06 funkci GUP, která zajištuje lokální aktualizace pro klienty v rámci lokality a tím šetří přenosové pásmo při šíření aktualizací. Systém antivirové ochrany je instalován na všech infrastrukturních serverech, pracovních stanicích a noteboocích lokalit a ústředí.

Systém je centrálně řízen a vyrozumíván pomocí SEP Manageru instalovaném na virtuálním serveru ústředí. SEP Manager má instalovanou databázi MS SQL na sdíleném SQL serveru. Na centrálním SEP Manageru je vytvořena struktura kontejnerů a rozdělena podle okresů, které se dále dělí na skupiny notebooky, servery a stanice; do kterých jsou zmiňované typy počítačů zařazovány s ohledem na jejich funkcionalitu. Na tyto skupiny (notebooky, stanice a servery) jsou aplikovány jednotlivé politiky AVO pro řízení a chování klientů SEP. Zařazení jednotlivých typů počítačů do přednastavených skupin a kontrola klientů, je v kompetenci správce dané lokality. Do kontroly souborů jsou zahrnuty všechny lokální disky a periferní zařízení. Toto nastavení platí pro pracovní stanice, notebooky a servery v lokalitách a ústředí.

Specifický režim kontroly dat v reálném čase i pomocí naplánované úlohy je přiřazen skupinám Servery, na které jsou aplikována pravidla beroucí v potaz fakt, že se může jednat o server obsahující databáze, takže v obou režimech kontroly jsou vyjmuty z kontroly adresáře obsahující databáze, resp. soubory nutné k provozu aplikace MS Exchange 2013 a vynechána kontrola souborů s koncovkami charakterizujícími databázové soubory. Viz. tabulky níže :

Tabulka přípon souborů vyjmutých z kontroly v reálném čase:

|  |
| --- |
| CAB |
| DAT |
| LD? |
| MD? |
| ED? |
| LOG |
| STM |

Tabulka výjimek ze skenování pro servery:

|  |
| --- |
| C:\Documents and Settings\All Users\Application Data\Mission Critical Software\OnePoint\... |
| C:\Documents and Settings\All Users\Application Data\Symantec |
| C:\WINNT\System32\SYSVOL |
| C:\WINNT\SYSVOL |
| C:\WINNT\System32\Wins |
| C:\WINNT\System32\DHCP |
| C:\WINNT\System32\Config |
| C:\WINNT\NTDS |
| C:\WINNT\System32\inetsrv |
| c:\Windows\Cluster |
| E:\USD\ASM\Library4.0 |
| C:\\_BizTalkConflicts\ |
| C:\\_BizTalkLogs\ |
| C:\\_BizTalkPorts\ |
| C:\ProgramData\Touchpaper\ |
| C:\ProgramData\LANDesk\ |
| C:\Program Files (x86)\LANDesk\ |
| C:\Program Files\LANDesk\ |
| C:\Documents adn Settings\All Users\Aplication Data\TouchPaper\ |
| C:\Documents adn Settings\All Users\Aplication Data\LANDesk\ |

Kontrola pracovních stanic, member serverů, stand alone serverů a notebooků je pro režim kontroly dat v reálném čase i pro režim naplánované úlohy, nastavena jednotně a tyto volby, nemá uživatel z pohledu běhu aplikace ani jednotlivých položek nastavení možnost změnit.

V případě kontroly na souborových systémech počítačů jsou stejně jako v případě poštovního provozu nastaveny velice přísné restrikce. Na SEP Manageru je na každou z výše jmenovaných skupin nastaveno v politice AVO, že v případě detekce zavirovaného souboru je jako první akce nastaveno jeho smazáni, v případě neúspěchu jeho uložení do karantény. Díky modulu pro kontrolu spywaru jsou identická nastavení použita i pro tento typ škodlivého obsahu.

Notebooky mimo organizace se liší oproti konfiguraci uvnitř organizace default konfigurací Firewallu. Pro možnosti změny firewallových politik podle toho, v jakém prostředí je notebook zapojen, jsou vytvořeny dvě lokace:

• mimo organizaci

• uvnitř organizace

Jako podmínka přepnutí mezi lokalitami se využívá ICMP request ze SEP Policy Managerů. Dostupnost Manageru pomocí ICMP requestu se ověřuje každých 30 sekund.

# Distribuce antivirových definic

SEP Manager se aktualizuje přímo z Internetu z Webu Symantecu a to každou hodinu. Po aktualizaci SEP Manageru budou aktualizace zasílány SEP klientům na serverech SIzz06 z funkcí GUP z které jsou aktualizovány virové definice SEP klientů. Stanice jsou nastavené, aby využívaly pouze GUPy, servery a notebooky v případě nefunkčnosti GUPu si berou definice přímo ze SEP Manageru. Aktualizace virových definic na klientech se provádí každé 4 hodiny.

Aktualizace virových definic notebooku, které jsou mimo organizaci jsou nastaveny přímo z Internetu z Webu Symantecu a to každou hodinu.

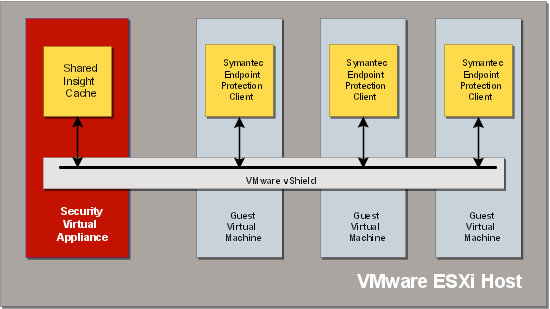
Záložně mají SEP klienti nastavenou aktualizaci z Liveupdate zrcadla umístěném na serveru.

# Antivirová ochrana VIRTUÁLNÍCH SERVERŮ

S masivním nasazením virtualizace je zavedena i antivirová kontrolavirtuálních serverů. Aby hypervizory, které provozují velké množství virtuálních strojů nebyly přetížené, výrobci AV přistupují k různým technikám, jak rozložit zátěž při skenování a kontrole filesystémů.

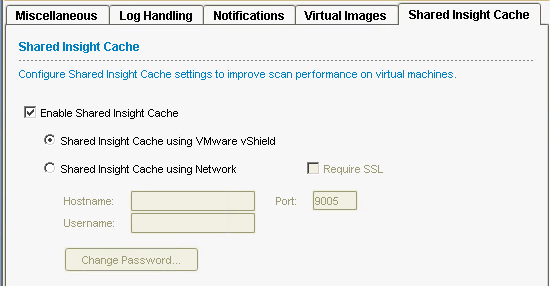
Z tohoto důvodu byla na každý vmware hypervizor nasazena virtuální appliance Symantec VA. Tato virtuální appliance udržuje ve své databázi (shared inside cache) otisky všech oskenovaných souborů a pokud je na jednom hypervizoru více serverů ve stejné verzi, skenuje z jejich filesystému jen soubory, které ještě ve své databázi nemá a ty, které byly změněny.

Princip funkce SVA:



Objekty virtuálních serverů jsou v rámci sep namageru umístěny v samostatných kontejnerech a aplikují se na ně politiky s nastavením, které umožňuje využití sdílené databáze na vmware infrastruktuře.

Nastavení politiky pro virtuální servery:



Kromě uvedené funkce jsou plánované skeny na virtuálních serverech načasovány nikoli na stejnou hodinu, ale pouze v rámci intervalu. Skeny pak neběží souč**asně a nezatěžují nadměrně hypervizory.**

# Odpovědnost jednotlivých činností

Antivirová ochrana elektronické pošty zodpovídají pracovníci oddělení 523.

Antivirová ochrana serverů a pracovních stanic odpovídají pracovníci oddělení 523 a administrátoři pracovišť ČSSZ.

# Schvalovací doložka a platnost standarDu

Standard byl schválen ………. dne ……….

.………………………………… podpis

Účinnost standardu od ……

Standard je platný do ……