Specifikace předmětu plnění

Požadované vlastnosti a technické parametry

Mezi základní parametry výběru antivirového řešení pro prostředí Policie ČR patří:

- nízké systémové nároky
- lokalizace řešení pro uživatelské stanice v českém a anglickém jazyce
- kvalitní detekce známých a neznámých bezpečnostních hrozeb
- rychlost skenování
- možnost centrální správy celého řešení
- plně automatizovaný proces antivirové kontroly a aktualizace antivirové databáze
- rychlá implementace nových verzí
- kvalitní implementační a běžná technická podpora

Požadované základní funkcionality:

1. rozsah antivirového řešení
    a/ rezidentní antivirová ochrana s real-time ochranou proti známým škodlivým kódům, tj. zejména, ale nejen: viry, červy, trojany, spyware, rootkity, spamem (blokování) i neznámými hrozbami
    b/ integrovaný firewall
    c/ systém se může skládat z komponent různých výrobců (na koncovém zařízení jeden softwarový produkt)

2. antivirové řešení musí podporovat
    a/ plánování automatického prověřování na hrozby
    b/ pravidelné aktualizace systému (automatické stahování aktualizací v pravidelných intervalech), skenovacích engine a datových řetězců s využitím automatické aktualizace pomocí sítě Internet a jejich přenos do oddělených (vnitřních) sítí
    c/ vynucení okamžitého update na vybraných klientech
    d/ sběr informací o virových nákazách a hrozbách z koncových stanic, logy skenování
    e/ pravidelné aktualizace klientů
    f/ okamžité automatické stažení a distribuce aktualizací na koncové stanice v případě potvrzené hrozby nejvyšší úrovně
    g/ možnost návratu na předchozí verzi antivirové databáze
    h/ rychlé základní prověření na hrozby na libovolném klientovi
    i/ historie prověřování na hrozby koncových stanic
    j/ možnost nastavení přípon prověřovaných souborů
    k/ nástroje pro vytvoření záchranného disku
    l/ jednotlivá zařízení musí být členitelná (zařaditelná) do skupin (např. servery, stanice, notebooky) a umět převzít zařazení z organizační struktury v Active Directory s tím, že každé skupině musí být možné přiřadit konfigurační profil, který

určuje nastavení antivirového systému tj. nastavení skenu v reálném čase, nastavení plánovaných skenů, výjimek pro neskenované soubory, atd.

3. antivirové řešení musí umožnit nasazení na
   a/ servery (včetně podpory technologie vShield pro vSphere)
   b/ uživatelské (koncové) stanice = stacionární počítače (PC, tenký klient) i notebooky
   c/ mobilní zařízení (např. chytré telefony, PDA,…)

4. antivirové řešení musí umožnit automatické nastavení místa aktualizací klienta podle síťového prostředí, např.
   a/ mimo síť
   b/ v síti Intranet
   c/ při připojení na Internet

5. požadavky na správu antivirového řešení
   a/ možnost centrální správy klientů
   b/ možnost centralizovaného dozoru dodržování vybraných (ze seznamu standardizovaných) politik
      - firewall
      - aktuálnost antimalware klienta
      - nastavení přístupových práv do konzole antimalware systému
   c/ škálovatelnost úrovní přístupů do správcovské konzole
   d/ správa aktualizací
   e/ možnost centralizované i decentralizované správy včetně:
      - deploymentu klientů
      - automatické distribuce nových verzí klientů
      - editace nastavení parametrů klientů na koncové stanici
   f/ snadné řešení přírůstkových aktualizací na PC nepřipojených k síti nebo PC v oddělených sítích (bez připojení k Internetu)
   g/ hierarchická topologie správy antiviru s delegováním práv administrátorů (např. u PČR úrovně: obvodní oddělení - územní obvody – kraj)

Rozsah implementační a standardní provozní podpory:

IMPLEMENTAČNÍ PODPORA

Implementační podpora, v případě dodání jiného řešení než stávajícího, zahrnuje poskytnutí pracovníků uchazeče licence, kteří zajistí

- zaškolení stanovených technických zástupců zadavatele licence s dodávaným Softwarem (školení bude probíhat v prostorách zadavatele, bude jednodenní, ve dvou termínech po 20 lidech),
- odinstalování stávajícího řešení antivirové ochrany ze všech serverů, koncových uživatelských stanic a mobilních zařízení v prostředí Policie ČR (celkový počet zařízení je cca 40 000, z toho cca 10 000 zařízení s nejednotným administrátorským přístupem není zařazeno do domény – samostatně stojící PC, izolované sítě, apod.),
- instalaci centrální řídící části dodávaného řešení antivirové ochrany, včetně zprovoznění stahování aktualizací virových bází do prostředí Policie ČR,

- instalaci krajských řídících částí dodávaného řešení antivirové ochrany a nastavení distribuce stažených aktualizací virových bází z centrální řídící části na krajské řídící části,
- nastavení základních politik pro antivirovou ochranu serverů, koncových uživatelských stanic a mobilních zařízení,
- instalaci antivirové ochrany na servery, koncové uživatelské stanice a vybraná mobilní zařízení (celkový počet zařízení je cca 40 000, z toho cca 10 000 zařízení s nejednotným administrátorským přístupem není zařazeno do domény – samostatně stojící PC, izolované sítě, apod.).

Help Desk v českém jazyce pro určené technické zástupce zadavatele v režimu 5x8 přímo telefonicky s technikem, který zná nasazované řešení.

Stávající antivirové řešení je založené na produktech společnosti ESET spol. s r.o.

STANDARDNÍ PROVOZNÍ PODPORA

- Help Desk v českém jazyce pro cca 40 určených technických zástupců zadavatele v režimu 5x8 přímo telefonicky s technikem, který zná nasazené řešení.
- Garantovaná snadná dostupnost aktualizací.
- Seznámení se zásadními změnami/opravami či novou verzí dodaného Softwaru pro všechny určené technické zástupce.
- FAQ - zajištění a zprovoznění přístupu na webu uchazeče.
- Školení bude probíhat v prostorách zadavatele nebo uchazeče, bude jednodenní, ve dvou termínech po 20 lidech.