Příloha č. 1 výzvy – Technická konfigurace

Minimální požadavky na AntiX software

Požadované konečné počty licencí Anti X software

700ks licencí AntiX software splňujících níže uvedené požadavky včetně 2 leté základní technické podpory do **31. 12. 2013** s nárokem na nové verze jednotlivých komponent systému.

Dodávka software pro AntiX ochranu

(pokud je v textu použit výraz antivirová ochrana, myslí se tím obecně ochrana před škodlivými kódy)

- Systém antivirové ochrany všech PC a serverů.
- Systém antivirové ochrany pro protokol SMTP a HTTP, HTTPS
- Systém antivirové ochrany SMTP pro MS Exchange 2003 a vyšší
- Poskytování aktualizací antivirových a IDS/IPS řetězců a podpory produktů v režimu 24 x 7.

Jednotlivé součásti Antivirové kontroly musí být „kompaktní“, tzn., že všechny požadované typy ochrany musí zajišťovat jediný výrobce.
Množství požadovaných licencí je uvedeno v příloze.
Konkrétní požadavky na součásti Antivirové kontroly jsou specifikovány v následujících bodech.

Dodávka AntiX kontroly

Minimální požadavky vyhlašovatele na Antivirové kontroly jsou následující:

Požadované funkcionality na straně pracovních stanic (PC, notebooky) – Endpoint Security:

- Antivirová ochrana s real-time ochranou proti Ad-ware, Spyware, rootkitům, keyloggerům a remotecontrol programům.
- Síťová IDS/IPS funkcionalita založená na generických i specifických signaturách hrozeb s trasováním a blokováním útočníků a možností tvorby a implementace vlastních signatur pro ochranu souborů, adresářů, služeb a registrů bez dodatečných nákladů na nákup SW.
- Funkcionalita personálního firewallu. Možnost definice firewall politiky na základě připojení - firemní síť, internet. Možnost definice firewall pravidla na konkrétní aplikaci.
- Možnost definice politiky pro spouštěné aplikace. Možnost definice více politik pro různé skupiny počítačů. Možnost vytvořit výjimku pro určité signatury, počítače.
- Možnost blokace wifi rozhraní v případě připojení přes LAN rozhraní.
- Automatické generování komunikačních pravidel bez nutnosti zásahu uživatele pro snadnou definici firemní politiky.
- Funkcionalita Network Access Control minimálně na straně klienta bez dodatečných nákladů na nákup SW.
- Aktivní štít pro ochranu proti útokům na nově zveřejněné zranitelnosti operačního systému a aplikací bez nutnosti instalovat bezpečnostní záplaty. Proaktivní detekce hrozeb - bez nutnosti aktualizací virové báze v krátkých několikaminutových intervalech. Technologie používající aktivní prevenci používáním heuristické analýzy a generických popisů zranitelností k zablokování nových pokusů o napadení slabých míst, a to ještě předtím, než dodavatel softwaru vydá opravu (zero-day threats).
- Systém musí monitorovat běžící aplikace a procesy, vyhledávat signatury jejich „špatného chování“ (proaktivní automatické analýzy chování aplikací a síťové komunikace) a následně na základě jejích výsledků detekce je podle pravidel blokovat nebo terminovat.

- Všechny součásti systému musí podporovat kontrolu integrity klienta (měření souladu s bezpečnostními zásadami - aktuálnost AV a běžící povinné procesy, apod.) a automatické akce pro dosažení shody - zjednání nápravy.
- Ochrana před zastavením služeb AV řešení, před odinstalací produktu, smazáním souborů a změnou nastavení
- SW distribuce musí mít schopnost aktualizace nejen obsahu (virové definice, signatury), ale i vlastního kódu klientů na nové verze a to z řídícího serveru na základě pravidel či příkazu.
- Navrhované řešení musí umožňovat reporting o všech aspektech fungování systému - online stav, stav distribuce verzí definic, nalezené hrozby, atd.
- Celý systém (všechny moduly) musí na základě automatické detekce umístění – na základě přítomnosti klienta v konkrétní části sítě definované IP adresou, bezdrátovým SSID, DNS příponou měnit svoje chováni a charakteristiku na základě předem definovaných modelů (pravidel) bez zásahu administrátora nebo uživatele.

Požadovaná podpora platforem operačních systémů:

Windows Server 2003 a novější ve všech jeho verzích, Windows XP SP2 a novější, pro verze 32-bit i 64-bit operačních systémů.

Požadavky na technické řešení:

Nabízené řešení musí splňovat zejména následující technické požadavky:

- rezidentní antivirová ochrana
- plánování úkolů kontroly virového napadení
- pravidelná aktualizace systému, skenovacích motorů a datových řetězců s využitím automatické aktualizace pomocí sítě Internetu a centrálního management serveru
- skenování archivních souborů
- více skenovacích mechanismů v rámci antivirového řešení z důvodu vyšší pravděpodobnosti zachycení nové infekce
- obsahuje subsystém proaktivní automatické analýzy chování aplikací a síťové komunikace a na základě jejích výsledků detekce a aktivní blokování hrozeb
- obsahuje síťové IDS založené na generických i specifických signaturách hrozeb, s možností aktivního blokování útočníka
- podporuje kontrolu integrity klienta (měření souladu s bezpečnostními zásadami - aktuálnost AV a běžící povinné procesy, apod.) a automatické akce pro dosažení shody - zjednání nápravy
- všechny funkce musí být dostupné prostřednictvím jediného centrálně spravovaného agenta a jediné konzoly
- Centrální správa ochrany koncových uživatelů
- Centrální antispamová a antivirová ochrana na protokolu SMTP
- Centrální webová ochrana HTTP, HTTPS, FTP
- SW distribuce musí mít schopnost aktualizace nejen obsahu (virové definice, signatury), ale i vlastního kódu klientů na nové verze a to z řídícího serveru bez přerušení provozu
- umožňuje reporting o všech aspektech fungování systému - online stav, stav distribuce verzí definic, nalezené hrozby, atd.
- systém musí chránit koncové body i na síťové úrovni proti propagaci síťových hrozeb
- systém musí obsahovat ochranu proti technikám rootkit
- systém musí obsahovat ochranu proti logování kláves a přetečení zásobníku
- podpora terminálových serverů - MS Terminal server a MS Remote Desktop Services
- Navržené řešení musí umožnit definovat alespoň základní filtrační pravidla TCP/IP protokolu pro zamezení vstupu nevhodného síťového provozu do OS serverů. Propustnost tohoto

lokálního firewallu nesmí degradovat výkonnost serveru, tj. musí být schopna práce v rychlostech 1 Gb/s.
- systém musí nabízet možnost implementace antivirového produktu v českém jazyce a s uživatelem musí komunikovat v českém jazyce

Požadavky na vlastnosti aktualizace:

- aktualizace je prováděna pomocí samostatného aktualizačního subsystému vybudovaného ve vnitřní síti zadavatele
- automatické PUSH i PULL aktualizace
- pokud nemá notebook konektivitu k aktualizačnímu serveru v síti zadavatele, aktualizuje se přímo z aktualizačních serverů uchazeče/výrobce
- automatické upozorňování na nové verze formou mailu
- systém musí podporovat automatické upozorňování na chybové stavy a automatický alerting
- přírůstková aktualizace nezatěžující přenosové linky (důraz bude kladen na minimální zátěž linek)
- aktualizace prostřednictvím protokolu http(s) (z důvodu snazší konfigurace a průchodu přes WAN linky)
- kontrola integrity datových souborů na vstupu (elektronicky podepsané datové soubory)
- kompatibilita přenášených datových souborů s AV ochranou na internetové bráně
- hierarchická distribuce datových souborů v síti z důvodu rozložení zátěže linek přenášenými daty
- automatická záloha systému aktualizací datových souborů pro případ, že selže primární aktualizace

Požadavky na centrální správu:

- Jednotná správa AV, Firewall, IPS, Device management, kontrola zdraví – pouze jedna konzole a jeden agent. Dále musí umožnit správu dalších prvků bezpečnosti, jako je centrální NAC s podporou 802.1x
- Centrální monitor událostí s možností detailního filtrování
- Správa klientů musí být realizovatelná centrálně (ale s ohledem na komunikaci po WAN).
- Zařízení musí být členitelné do skupin (servery, stanice, notebooky…) a umět převzít zařazení z organizační struktury v Active Directory. Možnost třídění a přidělování politiky spravovaných systémů na základě kritérií – velikost operační paměti, příslušnost ke skupině, IP rozsah, typ zařízení – server, stanice, notebook
- Každé skupině je možné přiřadit konfigurační profil, který určuje nastavení antivirového systému tj. nastavení skenu v reálném čase, nastavení plánovaných skenů a výjimek pro - neskenované soubory a musí být možné definovat různé parametry pro různé situace bez nutnosti zásahu administrátora např. dle rozsahu IP adres či adresy, připojení do VPN, připojení prostřednictvím wi-fi a podobně
- Řešení musí umožnit granularitu přidělování oprávnění, možnost definice více administrátorů a detailní nastavení jejich pravomocí:
    - tj. např. konfiguraci a pravidla celkového systému a profilů určují pouze centrální administrátoři (L1). To znamená, že politiku skenování skupin podle typu zařízení bude možné nastavovat pouze z profilu Admina L1.
    - Lokální administrátoři (L2, L3) budou mít práva pouze prohlížení, správy a začleňování zařízení do skupin (s definovanými profily) dle typu zařízení, přičemž je dodržena organizační hierarchie – administrátoři L3 mají uvedená oprávnění v rámci své organizační jednoty, administrátoři L2 mají uvedená oprávnění v rámci své organizační jednoty a podřízených organizačních jednotek, administrátoři L1 mají uvedená oprávnění v rámci své celé organizace

- vlastní centrální vyhrazená konzole pro správu AV řešení s možností její instalace na více stanicích a serverech, možnost web konzole
- centrální správa antivirového řešení založená na bezpečnostních politikách,
- elektronicky podepsané politiky (konfigurace) zasílané z konzoly na stanice z důvodu zvýšení bezpečnosti (zabránění modifikace AV řešení na klientech),
- komunikace stanic s centrální správou a administrátorem prostřednictvím protokolu http(s),
- spolupráce s AD, automatická instalace produktů po přidání počítače do sítě.
- reporty a dashboard – dynamické reporty zobrazující neustále aktuální stav, možnost definice vlastních reportů a dashboardu. Automatické zasílání reportů administrátorům.
- možnost služby vzdáleného dohledu nad antivirovou ochranou prostřednictvím vlastního zabezpečeného tunelu.
- notifikace administrátora o detekci hrozby, útoku, neúspěšné aktualizaci, detekci neznámého zařízení
- automatická aktualizace databází a záplat spravovaných produktů

Požadavky na rozšiřitelnost

Vyhlašovatel požaduje, aby předmět veřejné zakázky byl rozšiřitelný o následující komponenty, všechny musí být od téhož výrobce jako řešení nabízené v rámci zakázky.
Dodávka těchto komponent však není součástí této zakázky, vyhlašovatel pouze požaduje, aby o ně mohl v budoucnu případně dodané řešení rozšířit:

- řízení bezpečného přístupu přes VPN
- kontrola přístupu pomocí 802.1x
- auditing a správa dokumentů – možnost sledovat a identifikovat dokumenty, které jsou pouze pro vnitřní potřeby či mohou být kopírované
- nástroj pro šifrování dat, partitions nebo celých disků

Současné licence zadavatele

Výrobce a název vlastněného software	Počet licencí	Poznámka
SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER	396	KÚPK – konec podpory 10. 12. 2011
Symantec Endpoint protection	48	SÚSPK* Starý Plzenec a Rokycany
Eset – Nod 32 Antivirus	70	SÚSPK*
Grisoft AVG Antivirus	22	SÚSPK*

* SÚSPK - Správa a údržba silnic Plzeňského kraje, organizace zřízená Plzeňským krajem, jíž odbor informatiky Krajského úřadu Plzeňského kraje poskytuje ICT služby

V případě, že dodavatel nabídne jiné AntiX řešení, než stávající většinové od společnosti Symantec (SYMC PROTECTION SUITE ENTERPRISE EDITION), musí do své nabídkové ceny zahrnout i náklady na implementaci tohoto řešení.

Požadavky na nabídku

Dodavatel vytvoří nabídku obsahující popis nabízeného AntiX řešení, ze kterého bude zadavatel schopen zkontrolovat splnění minimálních požadavků. Dále bude obsahovat cenovou tabulku, ze které bude zřejmé, jaké položky tvoří celkovou nabídkovou cenu (ceny bez a včetně DPH). Tato tabulka bude obsahovat minimálně informace o počtu licencí, u kterých bude prodlužována podpora, a o počtu licencí, které budou dodány nově.