ЈП „ЗАВОД ЗА УРБАНИЗАМ ВОЈВОДИНЕ"
НОВИ САД

БРОЈ: ЈНМВ-1/07-543-8
ДАНА:02.04.2014.

Знак: ЉЉР
Веза: ЈНМВ-1/07

ПРЕДМЕТ: Одговор на постављено питање у вези јавне набавке мале вредности антивирус програма за заштиту сервера, број ЈНМВ-1/07

питање 1:

Можемо ли добити прецизну информацију за колико сервера а колико радних станица вам је потребан антивирус програм, да ли нудимо лиценцу за 1 сервер и 50 рачунара или само за сервер који има 50 корисника.

одговор 1:

Техничке карактеристике су прецизно наведене у Конкурсној документацији и понуђен програм мора у потпуности задовољити исте, које и овде наводимо:
„ТЕХНИЧКА СПЕЦИФИКАЦИЈА

1. Подршку за више оперативних система (32/64 битни) укључујући Linux, Windows XP, Windows 2000, Windows Server 2003, Windows Server 2003R2, Windows Vista, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Windows Server 2012 R2, Windows 7 и Windows 8 и 8.1.
2. Решење мора да подржава заштиту виртуалних машина (VMware, Hyper-V, Citrix) како на самим ВМ тако и директно на host-u без потребе инсталације клијента на свакој ВМ.
3. Централно управљање и администрирање решења из јединствене конзоле – управљање Windows и Linux рачунарима из јединствене конзоле. Централизована конзола треба да омогући увид у статус свих рачунара у мрежи и по потреби реинсталацију софтвера (нове верзије), дезинфекцију заражених рачунара као и оних код којих је на неки начин заустављено ажурирање, као и могућност централизованог наметања безбедносних полиса.
4. Могућност централизованог директног уклањања детектованих претњи, без посебног локалног покретања скенирања заштићеног рачунара. Уклањање претњи подразумева уклањање вируса, црва, тројанаца, adware и spyware софтвера, блокирање недозвољених апликација.
5. Решење мора да омогући да се послови администрације могу расподелити на више администратора са различитим административним правима (Role based administration).
6. Централизовано:
   - ажурирање антивирусних и осталих дефиниција
   - управљање надоградњом софтвера
   - управљање над клијетским firewall-ом из исте конзоле из које се управља и антивирусним решењем
   - извештавање и јављање о претњама путем:
   - Е маил поруке
   - desktop поруке
7. Могућност додавања у систем додатних конзола за централизовано управљање у

мрежи, по потреби и без посебног плаћања.

8. Комуникација између серверске и клијентске компоненте софтвера мора се вршити криптованим путем (SSL) од најмање 2048 бита.
9. Могућност графичког извештавања о раду софтвера који пружа прецизан увид у претње и друге догађаје који су се десили везано за антивирусну заштиту (креирања сумарних извештаја из исте контролне конзоле којом се администрира антивирусно решење).
10. Могућност филтрирања прегледа клијентских рачунара према жељеној категорији.
11. Велику брзину скенирања и малу хардверску захтевност, као и могућност заказаног скенирања радне станице у току њеног коришћења, без нарушавања перформанси рачунара. Антивирусни софтвер не сме да нарушава процес рада у смислу да перформансе радне станице или сервера не смеју бити битно деградиране (Load balancing scanning).
12. Аутоматско и мануелно скенирање по захтеву (on-demand), по приступу (on-access) и у претходно заказано време.
13. Подешавање интервала update-а са минималним временом од 5 минута.
14. Омогућавање минимизације протока који користи антивирусни програм при свом update-у као и подешавање приоритета при свом download-у.
15. Информације о клијентском делу антивирусног софтвера и њихове конфигурације (обављеном скенирању, откривању и уклањању вируса, као и о распореду ажурирања антивирусне базе) се могу складиштити, чувати и претраживати коришћењем базе података (MSDE/MSSQL...).
16. Решење мора да поседује функционалност аутоматске синхронизације са Microsoft ActiveDirectory сервисима, омогућавајући аутоматско додавање рачунара у контролну конзолу одмах по додавању рачунара у активни директоријум.
17. Решење мора да пружи појачану заштиту радних станица и фајл сервера од вируса, црва, тројанаца, adware и spyware софтвера, потенцијално нежељених апликација и промена registry базе.
18. Решење мора да пружи HIPS функционалност (Host Intrusion Prevention System), активно надгледајући процесе и проактивно спречавајући сумњиво понашање процеса (ZeroDay заштита).
19. Решење мора да пружи могућност дефинисања забране извршавања недозвољених апликација и блокирање дефинисаних апликација на заштићеним рачунарима, као и да омогући селективно допуштање или блокирање легитимних програма који утичу на пропусност мреже, доступност система и продуктивност корисника (Application control) уз помоћ предефинисаних категорија апликација (минимално 50 категорија).
20. Могућност дефинисања различитих нивоа права и степена контроле крајњег корисника над клијентским софтвером, укључујући и потпуну транспарентност (могућност дефинисања порука упозорења по жељи систем администратора).
21. Могућност додавања нових рачунара у систем антивирусне заштите без техничких ограничења, са роком пријаве нових рачунара на годишњем нивоу.
22. Право на аутоматско преузимање (update) са web страница произвођача програма преко "сервера" или сваког рачунара понаособ односно, право на освежавање отисака вируса током времена трајања лиценце.
23. Право на нове верзије програма у току трајања лиценце.
24. Решење мора бити оптимизовано за виртуално окружење.
25. Могућност централизоване контроле статуса сигурносних закрпа оперативних система и апликација (за десетину најпознатијих софтверских произвођача) – Patch Audit.
26. Функцију firewall-а на нивоу клијента.
27. Могућност контроле USB, IrDA, firewire, CD/DVD и осталих removable device уређаја (са опцијама Allow/Block/ReadOnly), са додатном могућношћу да једино унапред идентификовани преносни уређаји могу бити коришћени у компанијској мрежи.
28. Могућност on-line In-the-cloud провере репутације сумњивих фајлова и web сајтова (заштита од најновијих претњи без потребе за update-ом).

29. Могућност WEB заштите крајњег корисника (WEB скриптови, контрола приступа сајтовима према категорији), у компанијском окружењу и ван њега.
30. Решење мора да омогући URL контролу Web саобраћаја без обзира на врсту бровсера који се користи (подршка за IE, Firefox, Safari, Chrome, и Opera).
31. Могућност филтрације Web саобраћаја са предефинисаним категоријама неодговарајућих садржаја (минимум 14 категорија) и са могућношћу да се одобри, забрани или упозори приступ кориснику или групи корисника, и детаљне извештаје по корисницима. Мора постојати могућност дефинисања додатних категорија од стране администратора.
32. Заштита за Network Storage.
33. Могућност потпуне енкрипције фајлова као и појединачу енкрипцију датотека намењених слању мејлом или снимању на преносне меморије.
34. Заштита од неовлашћеног „цурења" информација по задатом обрасцу (потпуна контрола преноса осетљивих података на екстерне уређаје и путем других апликација), користећи опсежну глобалну листу осетљивих дефиниција података, које испоручује и ажурира сам произвођач софтвера (Data Loss Prevention). Мора омогућити могућност ручног проширења списка постојећих дефиниција и могућност самоучења корисника тако што ће га обавестити да је његов поступак у сукобу са политиком компаније и омогућити му да по потреби изврши сам ауторизацију поступка или га прекине на време.
35. Антивирусна и антиспам заштита долазног, одлазног и интерног имејл саобраћаја.
36. Централни карантин за спам пошту.
37. Лични карантин за спам пошту с могућношћу управљања сопственим карантином преко web конзоле, са креирањем allow и block листа.
38. Подршка за скенирање е-поште у реалном времену и скенирање датотека.
39. Антивирусна заштита за мејл сервер на нивоу заштите базе мејлова са скенирањем и дезинфекцијом постојећих мејлова у бази.
40. Подршка и интеграција са Microsoft Exchange 2003/2007/2010/2013 сервером.
41. Спречавање намерног или случајног „цурења" информација путем мејла, могућност праћења и филтрирања кључних речи (провера непожељних речи унутар електронске поште и .doc и .pdf attachmenta), типова фајлова и осталих осетљивих информација.
42. Подршку за коришћење вишеструких black/white листи при AntiSpam заштити.
43. Могућност примене URL категорија на линкове садржане у телу е-маила (Antispam заштита мора укључивати URL анализу и хеуристичку проверу).
44. Web базирани спам карантин за крајњег корисника, који подржава интеграцију са ActiveDirectory.
45. Једноставно креирање и контролисање правила за спољни и унутрашњи мејл саобраћај (дефинисање филтера са тежинским коефицијентима).
46. Антивирус провера на gateway-у, серверу и радним станицама.
47. Могућност постављања дистрибуиране архитектуре са редистрибутивним серверима за антивирус и antispyware решење.
48. Инкрементално освежавање malware дефиниција.
49. Сви купљени производи морају остати функционални и након истека уговореног периода одржавања.
50. Софтвер се испоручује у виду електронске лиценце.
51. Сва решења морају да буду од истог произвођача.
52. Лиценца треба да укључује и право коришћења антивирусног софтвера без функционалних ограничења и у истом броју за потребе кућног коришћења запослених у циљу повећања нивоа сигурности у компанији.
53. Период важења лиценци је 1 година.

Техничка подршка

- Цена мора обухватити комплетну инсталацију решења од стране испоручиоца на свим радним станицама које су предмет ове набавке.
- Цена мора обухватити 24*7 сертификовану техничку подршку и обавезно пост-продајно сервисирање од стране произвођача и испоручиоца софтвера путем телефона, е-маила и путем web-а, током трајања лиценце.
- Цена мора да обухвати обуку за администратора система, једанпут годишње и да траје минимално 1 дан. „

Што се тиче броја сервера и рачунара, у питању су три сервера и 47 радних станица. Понуђено програмско решење мора да обезбеди комплетну заштиту информационо техничке структуре, односно, сервера, радних станица, мреже каи и комплетне комуникационе инфраструктуре, а све у складу са дефинисаним техничким карактеристикама.

Потписи председника и чланова Комисије:

Аљоша Дабић, ел.техн - председник .....

Сандра Јавор Ивковић, дипл.прав.-члан .....

Љубица Розић, дипл.инж.агроек.-члан .....