„БДЖ – ТОВАРНИ ПРЕВОЗИ" ЕООД
ЦЕНТРАЛНО УПРАВЛЕНИЕ

ул. „Иван Вазов" № 3, гр.София 1080
тел. +359 2 932 45 05
факс: +359 2 987 79 83

www.bdzcargo.bdz.bg
e-mail: bdzcargo@bdzcargo.bg

ОДОБРЯВАМ:
ИНЖ. АНГЕЛ СТОЙНОВ
УПРАВИТЕЛ „БДЖ-ТП" ЕООД

ТЕХНИЧЕСКО ЗАДАНИЕ

За възлагане на обществена поръчка с предмет:
„Подновяване на срока на лицензии на антивирусен софтуер ESET Endpoint Protection Standart"

I. Съществуващо положение

В момента „БДЖ-Товарни превози" ЕООД разполага с 302 лицензa на антивирусния софтуер ESET Endpoint Protection Standart за защита на работните станции и сървърите.

II. Количествени характеристики

- Лиценз за антивирусен софтуер - 300 бр.;
- Лиценз за антивирусен софтуер за сървър MS Windows – 2 бр.;

Срок на валидност на антивирусните лицензи 2 год..

III. Изисквания към антивирусния софтуер

1. Корпоративна версия, базирана на клиент - сървърна технология
2. Съвместимост и поддръжка с операционни системи - Microsoft Windows 7,8,10 x32/x64;
3. Съвместимост и поддръжка на клиентската част на антивирусния софтуер с операционните системи - Microsoft Windows Server 2008 R2/2012 R2/2019 x32/x64;
4. Интелигентна защита в реално време и проактивен мониторинг за откриване и спиране на нови заплахи преди публикуване на традиционните вирусни дефиниции;
5. Статистика за хардуерна и софтуерна настройка на потребителските машини.
6. Създаване и управление на групи клиентски машини (според потребителски групи или според компютърни групи).
7. Да позволява централизирано конфигуриране, инсталиране и обновяване на вирусни дефиниции на антивирусния клиентски софтуер.

8. Интегрирани уеб-базирани графични отчети;
9. Централизирано следене на логовете на всички потребители.
10. Интеграция с MS Active Directory Services;
11. Автоматичен download на актуализациите и общ ъпдейт;
12. Създаване и налагане на политики за конфигуриране и управление на антивирусния клиентски софтуер
13. Възможност за създаване на политики за управление и конфигуриране на Firewall на антивирусния клиентски софтуер.
14. Възможност за създаване на списъци с одобрени и неодобрени програми и приложения за клиентските машини.
15. Възможност за обновяване от локален сървър, така и от сървър на производителя;
16. Възможност за отдалечено управление на офиси и отдалечено сканиране при поискване;
17. С възможност за настройки на защита, според изискванията на клиента;
18. Обща защита срещу вируси и шпионски софтуер;
19. Възможност за изключване на определени приложения или дискови масиви от сканиране в реално време, с цел бързодействието им, без това да нарушава защитата;
20. Възможност да се инсталират само определени компоненти от програмата;
21. Интелигентни настройки за по-бързо, по-малко на брой и по-кратки сканирания;
22. Защита от уеб атаки, които използват уязвимостта на софтуера;
23. Защита на имейл клиенти;
24. Антифишинг защита;
25. Проактивна, многослойна система за защита;
26. Блокиране на заплахи за браузъри, операционни системи и приложения;
27. Възможност за ползване на всички ново излезли версии през периода на валидност на лицензa;
28. Откриване и премахване на „бисквитки" (cookies) от Internet Explorer и Firefox;
29. Възможност за премахване на макро-вируси и възстановяване на документи;
30. Възможност за откриване на полиморфни и метаморфни вируси;
31. Възможност за сканиране на архивни файлове в познатите формати за компресия;
32. Възможност за карантина и изолиране на заразени файлове;
33. Възможност за възстановяване на системни файлове;
34. Използване на multi-thread технология и оптимизация за многопроцесорни системи;
35. Защита на собствените файлове на програмата;
36. Възможност за създаване на USB/CDROM Image даващ възможност за сканиране на системата в Offline режим;
37. Проверка за липсващи важни обновявания на операционната система;

38. Предупреждения за потенциална заплаха в ново свалени файлове и приложения преди те да бъдат отворени или инсталирани;
39. Предоставяне на подробна информация за откритите заплахи, вкл. какво са възнамерявали да правят заплахите и как са били елиминирани;
40. Да осигурява защита на работните станции;
41. Защита срещу keyloggers, автоматичен логин и попълване на форми;
42. Функционалност за одит на мрежата;
43. Да дава възможност за налагане на политики по отношение на шпионски и рекламни програми на принципа „приложение по приложение".

IV. Допълнителни изисквания

Участникът трябва да притежава оторизация от производителя или негово официално представителство за правото на продажба и поддръжка на програмния продукт ESET Endpoint Protection Standart в Република България.

[redacted]**Мартин Ангелов**
...кция „Финанси и администрация"

[redacted]**...инж. Надя Ганева**
...ИТ"

[redacted]**..... Магдалена Бозаджиева**
Гл. експерт „Системно осигуряване"