ПРИЛОЖЕНИЕ № 1
Образец

ТЕХНИЧЕСКО ЗАДАНИЕ

за възлагане на обществена поръчка с предмет „Осигуряване на корпоративна антивирусна, анти спам и други защити и филтрирания на входящия и изходящия трафик на локалната компютърна мрежа на МЗХ. Антивирусна защита на сървъри, персонални и преносими компютри собственост на МЗХ"

1. Предназначение на техническото задание

1.1. Предмет на техническото задание

Целта на този документ е да осигури корпоративна антивирусна, анти спам и други защити и филтрирания на входящия и изходящия трафик на локалната компютърна мрежа на МЗХ, както и антивирусна защита на сървъри, персонални и преносими компютри собственост на МЗХ.

1.2. Изисквания към предложението на участника:

Участникът предоставя оферта за хардуерно и софтуерно решения, чрез които ще осигури необходимите защити и филтрирания на входящия и изходящия трафик на локалната компютърна мрежа на МЗХ, както и антивирусна защита на сървъри, персонални и преносими компютри собственост на МЗХ.

1.3. Срок за стартиране изпълнението на поръчката - на 14.06.2013 г. изтича действащия в МЗХ договор и следва на 15.06.2013 г. изпълнителят да е стартирал изпълнението на услугата с оглед да се осъществи непрекъсваемост на антивирусната защита в сградата на министерството.

2. Софтуер за защита - изисквания:

2.1. Антивирусен софтуер

2.1.1. Основни функционалности:

Защита на сървъри и работни станции:

- Решението да защитава от вируси, червеи, троянски коне, шпионски и рекламен софтуер, rootkit заплахи и друг зловреден код.
- Проактивна защита от нови заплахи с помощта на евристичен модул за засичане.

- Възможност за контролиране за постигане на оптимално ниво на погрешно засечени файлове като заплахи (false positives).
- Сканиране във фонов режим.
- Интегриран персонален Firewall.
- Интегрирана host базирана IPS система.
- Да може да контролира USB устройства като флаш памети, външни дискове, MP3 плейъри и други носители на данни, като ги забранява или ограничава работата им без това да засяга работата с налични USB клавиатури, мишки и периферия.
- Да има контрол над приложенията - да може да се определя кои приложения може да ползва потребителя на машината и кои не, дори да са инсталирани. Да може да блокира опити за стартиране или инсталиране на непозволени приложения.
- Функционалностите: антивирус, firewall, host IPS, USB контрол и управление на приложенията да се инсталират с един агент по клиентските машини.
- Да има централизирана конзола, от която да се управляват всички функционалности.
- Да прави отдалечена инсталация по клиентските машини със средствата на централната конзола.
- Да може да се задават групи и да се прилагат различни политики за тях.
- Възможност за сканиране при достъп или поискване (on access и on demand сканиране).
- Възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции и т.н.).
- Изпращане на известия при възникване на предварително дефинирани събития (откриване на вируси, обновяване на дефиниции и др.).
- Възможност за централизирано, автоматично обновяване на антивирусните и host IPS дефинициите, както и на сканиращото ядро на продукта.
- Поддръжка на локални сървъри за разпространение на дефиниции и обновления.
- Възможност за инкрементални обновявания.
- Поддръжка на сканиране на Outlook и Outlook Express за вируси.
- Използване на multi-thread технология и оптимизация за многопроцесорни системи.

- Възможност за многослойно сканиране на вложени архивни файлове.
- Наличие на агент за бекъп на работните станции на файлово ниво и на имидж на системния дял на твърдия диск.
- Възстановяване от бекъп на цялата машина както на същия, така и на различен хардуер.
- Да е съвместима с операционните системи Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2003/2008;

Защита на MS Exchange:

- Да поддържа MS Exchange 2003, 2007 и 2010.
- Да защитава от вируси и спам.
- Да поддържа реализации във Vmware и Hyper-V виртуализирани среди.
- Възможност за Edge и Hub фокусирано сканиране за елиминиране на ненужно сканиране и намаляване натовареността при сканиране на дейта стор-а на Exchange.
- Да сканира в паметта и да поддържа multi-threading за многоядрени и многопроцесорни машини.
- Да има поне 99% ефективност в спирането на спам.
- Да има много ниско ниво на уловени по погрешка легитимни съобщения като спам (false postivies) - по-малко от 1 на 1.000.000.

Защита на web и mail трафик на входа на мрежата:

- Решение базирано на хардуерно устройство за филтриране на SMTP мейл трафик от вируси и спам.
- Решение от същия производител с интеграция с централната конзола за управление.
- Необходимост от минимална намеса от страна на администратора за поддържане на много високо ниво на улавяне на spam (да спира над 99% от spam и да има много ниско ниво на улавяне на легитимни съобщения като спам - под 1 на 1.000.000).
- Да притежава средства за подробен отчет и справки за случилото се (резултати от уловения спам в проценти, по дни и т.н.).
- Да има възможност за вдигане на 2ро виртуално устройство в във VMWare среда като резервно при проблем с физическото такова. Подготвен VMWare имидж на

виртуалното устройство да бъде стандартно подготвен от производителя и да се достави;

Защита от Web заплахи от вируси и ограничаване на достъпа до web страници и ресурси:

- Хардуерно решение за web филтриране за вируси, шпионски софтуер, botnets, и друг зловреден код.
- Решението да е от същия производител и да се интегрира с централната конзола за управление.
- Решението да може да ограничава достъпа до web сайтове (URL filtering) като това да може да се задава по потребителски групи.
- Възможност да открива, инспектира и блокира активни и неактивни botnet мрежи.
- Да притежава средства за подробен отчет (активността на потребителите, достъпените и блокираните сайтове, филтрираните вируси и т.н.).

2.1.2. Брой потребители на локалната компютърна мрежа в МЗХ:

1. Компютри, свързани в мрежа - 600 бр.
2. Компютри с инсталирана електронна поща — 600 бр.
3. Преносими компютри - 50 бр.
4. Сървъри - 30 бр.

2.2.Софтуер за управление

Софтуер за управление на защитата на ниво потребител при работа в активна директория (MS Windows Server 2003/2008 R2).

3. Софтуерната поддръжка трябва да включва задължително:

№	**Софтуерна поддръжка**	**Продължителност**
3.1.	Обновяване на дефинициите за антивирусно филтриране на входящия и изходящия трафик за устройствата от предложеното хардуерно решение от т. 1.2	12 месеца
3.2.	Обновяване на дефинициите за филтриране на нежелан e-mail трафик (спам) за устройство от т. 1.2	12 месеца
3.3.	Обновяване на дефинициите за забрана на достъпа до web страници по категории за устройство от т. 1.2	12 месеца
3.4.	Доставка, монтаж и въвеждане в експлоатация на оборудването, което е собственост на Изпълнителя.	В срок до 15.06.2013 г.
3.5.	Настройка на необходимите политики в предоставените устройства	До 10 работни дни след 15.06.2013 г.
3.6.	Първоначално обучение на екипа на дирекция „Електронно	До 20 работни дни след

	управление" за работа с хардуерното и софтуерното решение - 8 бр. служители - подписва се констативен протокол.	15.06.2013 г.
3.7.	Техническа и консултантска помощ, включително и системна поддръжка на хардуерното и софтуерното решение	12 месеца
3.8.	Периодично обучение на екипа на дирекция „Електронно управление" за работа с новостите в хардуерното и софтуерното решение - 8 бр. служители - подписва се констативни протоколи	3-ти, 6-ти, 9-ти месец от сключването на договора
3.9.	Техническа и консултантска помощ, включително и системна поддръжка на хардуерното и софтуерното решение	12 месеца

4. Изпълнителят доставя необходимото хардуерно оборудване в сградата на МЗХ и го предава чрез подписване с представители на възложителя на Предавателно - приемателен протокол № 1, съдържащ пълно описание на устройствата.

5. Място на изпълнение на поръчката:

гр. София, бул. „Христо Ботев" № 55 - сградата на Министерството на земеделието и храните.

6. Приемане изпълнението на поръчката - след подписването на протокола по т. 3.5 и след подписване на приемателен протокол № 2 между представители на възложителя и изпълнителя, констатиращ инсталирането и настройките на софтуера до 10 работни дни след 15.06.2013 г.

7. Начин на плащане - 100% от договорената цена ще бъде платена по банков път до 14 календарни дни след приемането на изпълнението на поръчката, посочено в т. 6.

8. След приключване на изпълнението на договора, оборудването доставено с протокол по т. 3.5 ще бъде предоставено обратно на изпълнителя след подписване на Предавателно - приемателен протокол № 3.