ПРИЛОЖЕНИЕ № 2

ТЕХНИЧЕСКО ЗАДАНИЕ

ЗА 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"

Изисквания към системата за защита на работни станции, сървъри и мобилни устройства от злонамерени атаки:

1. Общо описание:

- Съществуващи сървъри и работни станции:
  - 600 работни станции;
  - 50 мобилни компютъра;
  - 30 сървъра;
- Системата да осигурява защита чрез:
  - Антивирус за Windows, Linux, Sharepoint;
  - защита от шпионски и рекламен софтуер;
  - защитна стена и защита от атаки (host IPS);
  - контрол на устройствата;
  - сканиране на мрежата за външни, неоторизирани устройства (rogue detection);
  - предпазване изтичане на съдържание с криптиране на данни на цял диск, файлове или външни устройства;
  - поддръжка на функционалност Deep и AMT на Intel – опция;
  - защита на електронния пощенски трафик;
  - защита на Web трафика на потребителите.

2. Общи изисквания към системата – Windows/Linux:

- Дистрибуцията на различните функции да се осъществява централизирано през конзола за управление през единствен клиентски агент;
- Да поддържа инсталация във фонов режим (silent mode installation)
- Системата трябва да извлича информация от глобална база данни с дефиниции, с оглед предпазването на клиентските компютри и сървъри от нови и видоизменящи се заплахи;
- Да има функционалност за централизирано, автоматично обновяване на антивирусните и host IPS дефинициите, както и на сканиращото ядро на продукта. Компонентите за обновяване трябва да могат да се

дистрибутират от централизиран сървър към работни станции, които не са свързани с Интернет.

- Да сканира във фонов режим;
- Да може да сканира при достъп или поискване (on access и on demand сканиране)
- Да се интегрира с Active Directory с цел налагането на политики да се извършва спрямо потребителско име или група. Потребителските имена трябва да се виждат в отчетите на системата
- Да е съвместима с операционни системи Microsoft Windows XP / Vista / 7 / 8 / 8.1; Microsoft Windows Server 2003 / 2008 / 2009 / 2011 / 2012; Apple iOS 10.4+; Linux CentOS, Fedora, Debian, RHEL, Ubuntu, SuSE;
- Да предлага централизирано управление и наблюдение на всички звена от защитата;
- Централизираната конзола за управление да поддържа методи за автентификация – локална, сертификати, MS AD;
- Централизираната конзола за управление да поддържа конфигуриране на административни роли с различни нива на достъп. Да може да се конфигурира за акаунт – кои функции може да конфигурира, до кои части от интерфейса за управление има достъп.
- Централизираната конзола за управление да има Web интерфейс за пълна конфигурация или възможност за отдалечен достъп до пълната конфигурация;
- Централизираната конзола за управление трябва да може да управлява всички устройства (Linux, MAC, Android, Windows ...) и модули (защита на работни станции, защита на email, защита на Web), както и да получава и генерира отчети за работата има;
- Централизираната конзола за управление трябва да може да управлява и наблюдава в реално време работата на системата за сигурност за работните станции;
- за всички функции, за които не е отбелязано изрично друго да се поддържат само за Windows
- Кандидатът предлагащ решението трябва да е оторизиран за продажба инсталация и поддръжка на предложените решения;

3. Функции AntiVirus, AntiSpyware/AntiMalware – Windows:

- Проактивна защита от нови заплахи с помощта на евристичен модул за засичане;
- 0day защита от нови заплахи с помощта на облачна система за репутация;
- Облачната система за репутация трябва да поддържа репутация за IP, website, file;

- Възможност за контролиране нивото на засичане за постигане на оптимално ниво на погрешно засечени файлове като заплахи (false positives);
- Да може да блокира опити за инсталиране на приложения, да наблюдава записването и стартирането на програми в директории Windows, Program Files, Temp.
- Да може да сканира вложени архивни файлове;
- Да открива и блокира зловреден софтуер – Spyware, Adware, Remote Administration, Tools, Key loggers ...;
- Използване на multi-thread технология и оптимизация за многоядрени системи;
- На база облачен интелект системата трябва да може да определя нивото на риск на всеки сканиран файл, чрез изследване на следните файлови характеристики и съдържание:
  - ✓ Източник на файла
  - ✓ Колко нов е файла
  - ✓ Колко често се наблюдавава файла в Интернет
- В ежедневната си работа AV да не използва повече от 100MB RAM при сканиране;
- AV системата да е одобрена от Microsoft за работа с MS операционни системи;

4. Функции AntiVirus - Linux

- Откриване и блокиране на зловреден софтуер.

5. Функции host IPS:

- Проактивна защита от атаки;
- Защита от атаки на база дефиниции;
- Защита на операционната система от уязвимости преди инсталиране на update;
- 0day защита от нови заплахи с помощта на облачна система за репутация;
- Да разполага с интегриран персонален statefull Firewall.

6. Функции контрол на устройствата:

- Да може да контролира периферни устройства в това число флаш памети, външни дискове и други носители на данни, CD/DVD като ги забранява, ограничава работата им или само наблюдава използването в зависимост от потребителско име ли група в MS AD или в зависимост от ID и производител. Не трябва да се засяга работата на използваните от потребителя USB/PS2 клавиатури, мишки и периферия.

7. Функционалност сигирност за Sharepoint

- Откриване и блокиране на зловреден софтуер в Sharepoint съдържание
- 0day защита от нови заплахи с помощта на облачна система за репутация;
- Възможност за сканиране на съдържанието при достъп или поискване;
- DLP – разпознава над 400 документа и може да създава правила за да гарантира само оторизиран достъп до конфиденциална информация;
- Поддръжка на Sharepoint 2003 / 2007 / 2010 / 2013; Sharepoint Services 3;

8. Функции наблюдение и отчети:

- Възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции, станции с най-много вируси и т.н.)
- Изпращане на известия (email, SNMP trap) или предприемане на действия при възникване на предварително дефинирани събития (откриване на вируси, обновяване на дефиниции и др.);
- Отчетите трябва да са налични като минимум в следните формати: XML, HTML, CSV и PDF.
- Да има възможност за планово генериране на отчети и изпращането им по email или записване на Http/FTP;

9. Системата за защита на електронния пощенски трафик:

- Защита на минимум 1500 e-mail пощенски кутии;
- Да поддържа минимум 20 домейна;
- Да работи в Gateway/Proxy режим и да поддържа всички видове пощенски сървъри;
- Да защитава от DoS/DDos атаки пощенските сървъри с функции на ядрото на операционната система (Kernel Block);
- Да защитава от harvest атаки и SMTP уязвимости на последващите мейл сървъри;
- Да защитава от спам, фишинг, spyware, malware, вируси и червеи;
- Да има втори АВ скенер;
- Да може да сканира архиви;
- Да използва технологии за предпазване от СПАМ: облачна система за репутация, grey listing, RBL, SPF, BATV, DKIM, разпознаване на изображения, лексикален анализ, анализ на хедъри и др.;
- При избор за инсталация на повече от едно устройства за защита на електронна поща да има централизирана и обща карантина;
- Централизираната карантина да не изисква закупуване на нова операционна система, база данни или хардуер;

- Централизираната карантина трябва да предлага на всеки индивидуален потребител: портал за освобождаване на погрешно заподозрян спам, портал за въвеждане на бели и черни списъци;
- Централизираната карантина трябва да може да се локализира и изпращаните към потребителите съобщенията да са на български език;
- Да проверява e-mail трафика за Спам, Вируси, Compliance, DLP в изходяща посока (от вътрешни потребители към Интернет)
- Да предлага виртуализация. Например – за нов домейн или група да може да се използва отделен административен интерфейс, с нов IP за приемане и изпращане на поща с цел сегментиране на email трафика и с цел различни дирекции да могат да управляват само собствения си email трафик;
- Да има функции DLP – да може да се обучава за конфиденциално съдържания (да прави сигнатури за конфиденциални файлове и да използва регулярни изрази), да открива конфиденциални документи в email трафика и да блокира изпращането им;
- Да има функции Compliance – да може да проверява email трафика за изпълнение на международни стандарти и правила;
- Да използва LDAP за проверка на потребители и рутиране на email съобщения;
- Да притежава средства за подробен отчет и справки за случилото се (резултати от уловения спам в проценти, по дни и т.н.);
- Да притежава средства за отчетност, които да позволяват анализ на получените съобщения – час, дата, изпращач, получател, IP на сървър, използвани филтри за обработка на съобщението и т.н.;
- Да поддържа TLS, PGP, S/MIME;
- Да разполага с Web портал за криптирано доставяне на съобщения – съобщения, които системата разпознае като конфиденциални да не излизат в Интернет, а да се четат посредством секретен Web линк;
- В случай на потребност от инсталация на още едно устройство с цел резервираност да бъдат предвидени необходимите лицензи;
- Да може да работи в режим на резервираност Clustering;
- Да поддържа централизирано управление на резервирания Cluster без нужда от допълнителен хардуер/софтуер/лицензи;
- Да се предвиди Анти Спам и Анти Вирус проверката да бъде резервирана – в случай на отпадане на устройството пощенският сървър и клиентите да продължат да получават проверена за Спам и Вируси поща;
- Кандидатът предлагащ решението трябва да е оторизиран за продажба инсталация и поддръжка на предложените решения;

10. Системата за защита на Web трафика на потребителите

- Сканиране на протоколи HTTP,/HTTPS и FTP;
- Сканиране на потребителския трафик, откриване и блокиране на зловреден софтуер;
- Използва два Анти Вирус скенера;
- Сканиране на Web 2.0 приложения, Сканиране на Flash, JavaScript, Java, ActiveX, Visual Basic, Windows libraries и др за откриване на зловреден код. Изрязване само на подозрителната част от сайт и визуализиране на останалото на потребителя;
- Сканиране на MS Office документи, сканиране на PDF за откриване на зловреден код или DLP Compliance;
- Разпознава блокира и рапортува над 1000 Web приложения;
- Оптимизация на сканирането за realtime streaming media трафик;
- Възможност за филтриране на типове файлове, които да могат да се разменят през в сканирания протокол;
- Възможност за филтриране на команди, които да могат да се изпълняват в сканирания протокол GET, POST, PUT. DELETE …
- Instant message поддръжка – Yahoo, MSN, Windows Live, XMPP (Google, Facebook, …)
- URL филтриране с над 95 категории;
- Динамичен класификатор за неизвестни сайтове;
- Действия за сайтове – Allow, Block, Time Quota, Volume Quota, Coaching;
- Интегрира се с MS AD за създаване на правила по потребител/група; Рапортува потребителски имена в отчетите; Автоматично разпознава потребител след като се е логнал в AD, не изисква втори SignOn за да може потребител да има Интернет;
- Режими на работа – proxy и transparent bridge/router;
- В случай на потребност от инсталация на още едно устройство с цел резервираност да бъдат предвидени необходимите лицензи;
- Да може да работи в режим на резервираност Clustering;
- Съобщенията за грешка и аларма към потребителите да могат да са на български език;
- Поддръжка на ICAP, WCCP;
- Кеширащо прокси за вече проверено съдържание;
- Да поддържа централизирано управление на резервирания Cluster без нужда от допълнителен хардуер/софтуер/лицензи;
- Извършване на филтриране според корпоративните правила независимо дали крайният потребител се намира в рамките на министерството или в Интернет. За филтрирането на потребителите в Интернет да бъде предвидено резервиране на услугата т.е. ако потребителя има Интернет той да бъде филтриран по корпоративните правила.

- Кандидатът предлагащ решението трябва да е оторизиран за продажба инсталация и поддръжка на предложените решения.

11. Изисквания за инсталация и конфигурация

Изпълнителят да монтира и конфигурира предоставените от него устройства и ги предава на МЗХ чрез подписване на Предавателно – приемателен протокол №1, съдържащ пълно описание на устройствата от представители на възложителя, както и продукти за крайно ползване в сградата на МЗХ;

12. Обучение

Изпълнителят да осигури обучение на поне трима експерти от дирекция АОЕУ, отдел ЕУ за боравене с платформата на продукта/продуктите, който/които ще предоставят.