"БДЖ – ПЪТНИЧЕСКИ ПРЕВОЗИ" ЕООД
ЦЕНТРАЛНО УПРАВЛЕНИЕ

ул. "Иван Вазов" № 3, София 1080, България
тел.:(+3592)987 8869
bdz_passengers@bdz.bg
www.bdz.bg

ОДОБРЯВАМ:

Биляна Христо

Заличено на основание регламент 2016/679

И.д. Директор „Финанси"

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

За възлагане на обществена поръчка с предмет:

Предоставяне на 1000 броя лицензи за антивирусна програма от ново поколение (EDR).

1. Обща информация.

Предложеното решение трябва да предоставя ефективна защита срещу всички съвременни заплахи, като трябва да могат да бъдат защитавани потребителски операционни системи MS Win 10, MS Win 11 и сървърни операционни системи MS Windows Server 2016 и по нови.

Срок на лицензите – 24 месеца от датата на сключване на договор.

2. Минимални технически изисквания, функционалности и възможности.

Предложеното решение трябва да притежава/отговаря на следните минимални технически изисквания, функционалности и възможности:

2.1 Защита:

- Възможност за сканиране в реално време – ръчно или автоматично (което да подлежи на настройка);
- Възможност за блокиране на връзката до компрометирани "Command&Control" домейни;
- Възможност за отдалечена диагностика, директно през конзола, на всяка защитена машина в мрежата;
- Сканиране на преносими носители на информация при тяхното включване и изключване на работна станция;
- Сканиране на вложени архиви;
- Възможност за карантиниране на работни станции (до обновяване до последни антивирусни дефиниции);
- Да предоставя възможност за оценка и блокиране на опасни сайтове;
- Блокиране на определено съдържание от непознати или подозрителни сайтове на база на своите дефиниции (например скриптове и и Fileless атаки);
- Предпазване от опити за автентикация от устройства, имитиращи клавиатура;
- Предпазване от опити за криптиране на информация включително и от непознати крипто-вируси и възстановяване на повредената информация от тях;
- Защита на критични онлайн услуги - защитава потребителите от зловредна активност, докато достъпват онлайн банкиране и други критични за бизнеса сайтове;
- Възможност за анализ на риска на крайната точка - идентифициране на грешни конфигурации на OS и уязвим софтуер;
- Възможност за мрежова изолация на крайна точка директно от конзолата – спиране на мрежовия достъп на машината, запазвайки връзката само към сървъра за управление;
- Възможност за визуализация на инциденти - графично представяне на веригата на атаката в рамките на крайната точка, което включва изобразяване на връзките между процеси, създадени файлове, промени в регистри и мрежови връзки, инициирани от устройството;
-Възможност за визуализация на общ преглед за конкретен инцидент, като този преглед включва важни моменти от инцидента (highlights), броя на крайните устройства (машини,сървъри) засегнати от инцидента, оценка на важността на инцидента и др.

-Възможността за визуализацията на инциденти трябва да съдържа като отделни компоненти – графика показваща устройството от което е започнал инцидента, кой процес е идентифициран като зловреден, и какъв е мащаба на инцидента (колко и кои крайни точки са засегнати), таблица с детайлно описани действия, които са идентицирани като зловредни техники и технологий по MITRE ATT&CK матрицата и компонент за реакция показващ какви действия са необходими, в процес на изпълнение, изпълнени, пропуснати или всички действия;

- Възможност на всеки отделен инцидент да се задава ръчно приоритет, статус и техник/администратор който разглежда инцидента;

- Възможност за търсене на исторически данни в рамките на организацията за конкретни индикатори (IOCs) – файлови хешове, имена на процеси или командни редове;

- Възможност за сигурна терминална връзка (command-line interface) към всяка защитена машина за събиране на данни, спиране на процеси и навигация във файловата система;

- Възможност за автоматично или ръчно изпращане на подозрителни файлове, открити на крайната точка, към изолирана среда за анализ на поведението и получаване на доклад за verdict (зловреден/безопасен);

2.2 Управление:

- Централизирано управление (Management Console), което да се инсталира в мрежата на БДЖ или да може да се използва като облачна услуга, със същата функционалност;

- Възможност за интеграция с Активна Директория;

- Възможност за отдалечена инсталация на Софтуера върху работни станции в мрежата;

- Възможност за откриване на нови и незащитени работни станции в мрежата .

- Автоматично и централизирано обновяване на версиите на продукта и на вирусните дефиниции (минимум 4 часа или по-често);

- Възможност за ръчно обновяване;

- Отдалечено изпълнение на почистващи действия върху заразена работна станция;

- Възможност централно дефиниране на black list за достъп до уеб сайтове Контрол и управление на уеб потреблението, като да има възможност за забраняване на неуместни сайтове;

- Централизирано управление на преносимите устройства, свързвани към работни станции в мрежата (USB, външен диск, CD, DVD и др.);

- Възможност за изключване/деактивиране на USB/CD/DVD/Bluetooth (и др.) периферия/портове/устройства;

- Възможност за създаване на списък с „доверени “ устройства (всички извън него да не се допускат);

- Да предоставя възможност за автоматично управление на софтуерни обновявания на Windows и други софтуери от трети страни, до последната им версия, с цел да се избегнат уязвимости, без това да изисква инсталацията на допълнителен софтуер;

- Да притежава мониторинг и гарантиране на отчети с детайлна информация;

- Възможност за известия по електронна поща;

2.2.1 ***Други:***

- Предложеното решение, трябва да включва поддръжка на MS Win 10, MS Win 11, сървърни операционни системи MS Windows Server 2016 и по нови, MacOS и Linux.

- Възможност за периодично автоматично сканиране на работните станции и сървърите за липсващи обновления на сигурността;

- Възможност за обновяване както на операционната система (Windows/Linux), така и на най-често използваните приложения от трети страни (Adobe, Java, Firefox, Zoom и други);

- Възможност за настройка на графици за инсталиране на patching, както и опция за автоматично или ръчно одобряване на обновленията;

- Детайлни доклади за статус на уязвимостите – кои пачове са инсталирани, кои липсват и кои инсталации са били неуспешни;

Забележка: Всеки участник трябва да предостави документация (user manual), доказваща покриването на поисканите функционалности.*

Изготвил:

. **Георги Георгиев**

Ръководител отдел „ИТ и АО“