ОБҐРУНТУВАННЯ

технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(відповідно до постанови Кабінету Міністрів України від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами)

Найменування предмету закупівлі, код ДК 021:2015	Розмір бюджетного призначення	Очікувана вартість предмета закупівлі	Обґрунтування розміру бюджетного призначення, очікуваної вартості предмета закупівлі	Обґрунтування технічних та якісних характеристик предмета закупівлі
Закупівля послуг з постачання програмного забезпечення та його налаштування, подовження технічної підтримки від виробника, що входить до комплексу по захисту кінцевих користувачів та мережі у складі модулів Symantec Messaging Gateway та FortiGate601E **(72260000-5 Послуги, пов'язані з програмним забезпеченням)**	**2 349 906,00 грн**	**2 349 906,00 грн**	Розмір бюджетного призначення визначений в межах видатків, передбачених кошторисом на 2023 рік Секретаріату Уповноваженого Верховної Ради України з прав людини за бюджетною програмою КПКВК 5991010 «Парламентський контроль за додержанням конституційних прав і свобод людини» по КЕКВ 2240 "Оплата послуг (крім комунальних)". Очікувана вартість предмета закупівлі визначена відповідно до Методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Секретаріату Уповноваженого Верховної Ради України з прав людини 30 листопада 2020 року № 154.15/20. Для розрахунку очікуваної вартості було застосовано метод порівняння ринкових цін, використано інформацію щодо ціни на послуги отримані в результаті ринкових консультацій.	1. Технічні вимоги до подовження технічної підтримки від виробника до модулю Symantec Massaging Gateway: 1.1. Вимоги до Системних функцій та характеристик програмного забезпечення: 1.1.1. Можливість виявляти вхідні повідомлення (листи) як спам, вірус та можливість застосовувати до них ряд дій: видалити, помістити в карантин, змінити заголовок листа, сповістити користувачів/адміністраторів, тощо; 1.1.2. Захист від фішингово вмісту та технологій, що крадуть особисті дані користувачів; 1.1.3. Можливість затримання підозрілих файлів в карантині на вказаний проміжок часу, або до появи оновлених вірусних сигнатур; 1.1.4. Блокування експлойтів в поштових повідомленнях; 1.1.5. Аналіз поштових вкладень та архівів з можливістю застосування відповідних дій; 1.1.6. Ідентифікація потенційно небезпечних скриптів; 1.1.7. Категоризувати вхідну пошту та додавати заголовок до повідомлення, як: новинні, маркетингові розсилки, тощо; 1.1.8. Автоматичне оновлення антивірусних баз за розкладом або за запитом, з сайту виробника або з вказаного адміністратором джерела оновлень; 1.1.9. Застосування чорних\білих списків IP адрес, доменів, відправників, тощо; 1.1.10. Можливість ідентифікації масової розсилки; 1.1.11. Наявність централізованого спам карантину поштових повідомлень; 1.1.12. Можливість управління параметрами зберігання листів в поштовому карантині, об'ємом зберігання і періодом зберігання повідомлень в поштовому карантині; 1.1.13. Можливість індивідуального перегляду повідомлень в карантині для кожної контрольованої поштової адреси доступ (кожен користувач повинен мати доступ лише до своїх листів, що знаходяться в карантині), включаючи можливість досилання поштових повідомлень з карантину; 1.1.14. Можливість вивільнення листів з карантину без входу в інтерфейс карантину; 1.1.15. Можливість завдання індивідуальних для кожного користувача чорних та білих списків відправників; 1.1.16. Підтримка технологій Email автентифікації – Domain Key Identified Management (DKIM), Sender Policy Framework (SPF); 1.1.17. Робота з великою кількістю внутрішніх доменів, не менше 100 доменів; 1.1.18. Маскування внутрішніх адрес (address masquerading). 1.2. Вимоги до функціональних можливостей Анти-спам захисту програмного забезпечення: 1.2.1. Наявність багаторівневого спаму-фільтру; 1.2.2. Можливість використання додаткових джерел антиспам; 1.2.3. Можливість обриву та відхилення SMTP - сесії (SMTP defer / SMTP reject) при виявленні спаму; 1.2.4. Оновлення антиспам описів та списків репутації не рідше 1 раз в 30 хвилин;

				1.2.5. Застосування різних дій в разі виявлення спам-розсилки (блокування, відстрочення, додавання заголовка, тощо); 1.2.6. Глибока інспекція заголовку повідомлення (email header). 1.3. Вимоги до функціональних можливостей Захисту по репутації: 1.3.1. Аналіз репутації та вмісту; 1.3.2. Використання глобальної репутації від виробника для детектування спаму (репутація IP адрес, DNS адрес); 1.3.3. Накопичення локальної репутації відправників і подальшого її використання для детектування спаму; 1.3.4. Обмеження пропускної спроможності на мережевому рівні від серверів з поганою репутацією; 1.3.5. Можливість автоматичного пропуску антиспаму-перевірок для серверів з «хорошою» репутацією; 1.3.6. Захист від підроблених адресів (joe job attack, backscatter attack); 1.3.7. Утримання підозрілих листів до ухвалення рішення зі сторони адміністратора системи (офіцера безпеки); 1.3.8. Підтримка інтеграції з розширеною системою DLP за допомогою MTA (Mail Transfer Agent) транспортного агенту; 1.3.9. Визначення декількох вердиктів для одного повідомлення одночасно (наприклад, видалення вкладення, додавання заголовка та відправка в архів). 1.4.1. Сигнатурний антивірусний аналіз; 1.4.2. Захист від вірусів та вірусних атак (після здобуття визначеної кількості вірусів за вказаний проміжок часу повідомлення перестануть прийматися від цього відправника протягом вказаного проміжку часу); 1.4.3. Застосування різних дій (видалення, відстрочення відправки, тощо) з небезпечним вмістом. 1.5. Вимоги до функціональних можливостей Захисту на основі аналізу вмісту (Content filtering): 1.5.1. Підтримка регулярних виразів для аналізу контенту; 1.5.2. Підтримка аналізу вмісту за ключовими словами, завдання порогу кількості входжень ключового слова; 1.5.3. Видалення активного вмісту (макросів, Java, Flash) з файлів типу Microsoft Office (doc, docx, xls, xlsx) та PDF файлів; 1.5.4. Виявлення та блокування зашифрованих файлів, до яких не може бути підібрано пароль; 1.5.5. Визначення максимальної кількості вкладень у повідомлені; 1.5.6. Визначення типів файлів та розширення файлів, які потрібно сканувати та блокувати. 1.6. Вимоги до функціональних можливостей Захисту від просунутих загроз, від націлених атак: 1.6.1. Можливість захищати вхідні повідомлення (листи) від націлених атак завдяки видаленню загроз «нульового дня» з вкладень PDF і документів MS Office за допомогою вбудованої технології. 1.7. Вимоги до функціональних можливостей Управління, реєстрації (Logging) та звітності (Reporting): 1.7.1. Наявність єдиної консолі управління всіма модулями\компонентами системи; 1.7.2. Наявність ролевого доступу для адміністрування та аналізу; 1.7.3. Підтримка інтеграції з LDAP, MS AD для можливості автентифікації та перевірки наявності користувачів (відправників\отримувачів); 1.7.4. Консоль управління повинна забезпечувати доступ до інформації про параметри стану засобів захисту, перегляд журналів подій, у тому числі і про дії адміністраторів системи. Журнал безпеки повинен зберігати інформацію заданий термін, бути недоступним для редагування адміністратором додатка, забезпечувати детальність аж до конкретних дій глобального адміністратора системи, так і ролей/груп; 1.7.5. Наявність вбудованих засобів резервного копіювання/відновлення системи (з можливістю створення повної або часткової копії даних); 1.7.6. Підтримка роботи, як на фізичному пристрої, так і у віртуальному середовищі VMware та Hyper-V; 1.7.7. Реєстрація системних подій пов'язаних з роботою системи; 1.7.8. Реєстрація подій, пов'язаних з виявлення вірусів, результатами

				фільтрації спаму, роботи протоколів POP3, SMTP, інших ; 1.7.9. Підтримка можливості формування звітів на основі зібраних даних; 1.7.10. Підтримка створення власних шаблонів звітів; 1.7.11. Підтримка визначення автоматичних дій на виникнення вибіркових подій безпеки; 1.7.12. Підтримка групування подій по джерелу, адресатові, користувачеві або типові події безпеки; 1.7.13. Автоматичне створення звітів за періоди і їх автоматична розсилка за розкладом адміністраторам або іншим користувачам; 1.7.14. Можливість експортування звітів в PDF, CSV, HTML; 1.7.15. Детальне протоколювання подій фільтрації пошти з можливістю пошуку по журналу по різних параметрах (відправник, одержувач, IP адреса відправника, щодо); 1.7.16. Підтримка передачі журнальної інформації на віддалений Syslog-сервер; 1.7.17. Система має надавати детальний звіт щодо поштової статистики, виявлених загроз, поточних сесій, top-користувачів. 2. Технічні вимоги до подовження сервісу технічної підтримки (FortiCare Premium) існуючого обладнання FortiGate601E на 12 місяців за схемою 24*7 та продовження ліцензування функціональності сервісів безпеки (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc) на 12 місяців. Кількість- 2 од. 2.1. Продовження не менше ніж на 12 місяців сервісу технічної підтримки виробника; 2.2. Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7; 2.3. Постійний авторизований доступ до сайту виробника 24*7; 2.4. Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc); 2.5. Отримання основних та проміжних релізів програмного забезпечення; 2.6. Можливість реєстрації сервісних випадків в режимі 24*7; 2.7. Доставка і заміна запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника). 3.Вимоги до підтримки та придбання: 3.1. Весь об'єм програмного забезпечення, який постачається, повинен мати технічну підтримку виробника на термін не менше ніж 12 (дванадцять) місяців; 3.2. Право використання запропонованого програмного забезпеченням повинно бути доступно на основі тимчасового використання (не менше року); 3.3. Наявність служби технічної підтримки від виробника для усіх модулів комплексу; 3.4. Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7; 3.5. Постійний авторизований доступ до сайту виробника 24*7; 3.6. Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки; 3.7. Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.

Директор Департаменту господарського забезпечення **Євгеній СІРУК**

Дата оголошення про проведення конкурентної процедури закупівель: 22 жовтня 2024

Номер оголошення про проведення конкурентної процедури закупівель: **UA-2024-10-22-015057-a**