ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з ДК 021:2015 код 72260000-5 «Послуги, пов'язані з програмним забезпеченням» (Послуги у сфері інформатизації з постачання програмного забезпечення для роботи з електронною поштою на виконання п. 4.4. завдань регіональної програми інформатизації "Електронна Дніпропетровщина" на 2020–2022 роки)

1. Замовник

Департамент цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської облдержадміністрації.

2. Підстави закупівлі

Закупівля здійснюється відповідно до пункту 4.4. завдань регіональної програми інформатизації «Електронна Дніпропетровщина» на 2020–2022 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 25 жовтня 2019 року № 506-18/VII.

Метою закупівлі є забезпечення програмним продуктом поштового серверного обладнання електронного комунікаційного центру (ЕКЦ) області корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації для захисту електронної пошти відповідно до вимог комплексної системи захисту інформації.

Відповідно до вимог комплексної системи захисту інформації необхідно здійснювати дієві заходи щодо захисту системи електронного листування від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп'ютерного обладнання та захисту інформації на них, а саме: забезпечувати багаторівневий захист від усього спектра загроз, що передаються електронною поштою, допомагати виявляти та запобігати атакам через електронну пошту, включаючи спам, фішинг, розсилку шкідливих програм та посилань, заміну відправника та компрометацію корпоративної електронної пошти (BEC).

Одним з найдієвіших заходів для вирішення вищезазначених завдань є встановлення відповідного програмного забезпечення на ЕКЦ області.

3. Очікувана вартість предмета закупівлі: 430 000 грн з ПДВ (обласний бюджет).

Очікувана вартість сформована на підставі запиту безпосередньо до виробника програмної продукції, самостійного аналізу цін на аналогічні за технічними характеристиками типу програмної продукції через мережу Інтернет та в електронній системі закупівель Prozorro, а також з урахуванням необхідності економії бюджетних коштів в умовах військового стану.

4. Технічні та якісні характеристики предмета закупівлі

Найменування програмного забезпечення	Кількість, од.
Програмне забезпечення FortiMail-VM virtual appliance for all supported platforms. 2 x vCPU cores	1
Програмне забезпечення FortiMail-VM02 1 Year 24x7 FortiCare and FortiGuard Base Bundle Contract	1

Загальні вимоги

- Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем або ліцензій, то все це

має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки

- Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення
- На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від виробника

Архітектура та форм-фактор

- Система повинна забезпечувати захист корпоративної поштової системи шляхом аналізу повідомлень електронної пошти з метою виявлення спаму та забезпечення антивірусного захисту
- Система має поставлятись як віртуальна машина (VM), що буде встановлюватися на відповідний сервер з системою віртуалізації, що надаються замовником

Продуктивність

- Продуктивність маршрутизації електронної пошти з антивірусною та антиспам перевіркою на типових повідомленнях розміром 100 KB - не менше ніж 55 000 за годину
- Підтримка не менше ніж 70 поштових доменів, які будуть захищатися системою

Режими роботи системи

- MTA relay (gateway)
- Поштовий сервер + MTA relay
- Прозорий MTA relay (transparent)
- Статична маршрутизація
- Типи інтерфейсів: фізичний, VLAN, loopback
- Відмовостійкість на рівні інтерфейсів (redundant interface або агрегація інтерфейсів)
- Формування асоціації (linked) між інтерфейсами, моніторинг стану цих інтерфейсів (up чи down) та підтримка в автоматичному режимі однаковості їх станів (усі up, або усі down)

Системні функції

- Забезпечення фільтрації вхідної та вихідної електронної пошти, перевірки на антиспам, антивірус, контентний захист, захист від невідомих та просунутих загроз
- Підтримка протоколів HTTPS, SMTPS, SMTP over SSL/TLS, SSH, IMAPS та POP3S
- Підтримка перевірки сертифікатів SMTP-серверів під час встановлення з ними SMTP-сесії
- SMTP-автентифікація за допомогою LDAP, RADIUS, POP3, IMAP
- Перевірка адреси одержувача (recipient address verification)
- Шифрування повідомлень на основі S/MIME стандарту
- Заміна адреси одержувача будь-якого “зараженого” повідомлення або спам-повідомлення, на іншу адресу, наприклад, адміністратора (rewrite recipient email address)
- Архівування вхідних та вихідних повідомлень на локальному диску або на мережевому сервері

Анти-спам сервіси

- Перевірка на основі поведінки сервера, що відправляє повідомлення (greylisting)

- Перевірка повідомлень на основі бази адрес Spam DNS (domain name, ip-address) відправників пошти
- Перевірка повідомлень на основі бази Spam URI аналізуючи посилання URI (web sites, URL) у повідомленнях
- Перевірка повідомлень на основі сторонніх баз Spam DNS та Spam URI
- Перевірка повідомлень на основі бази Spam Checksum вираховуючи контрольну суму повідомлення (checksum)
- Перевірка повідомлень на основі Bayesian бази, аналізуючи слова у повідомленнях (email header та body)
- Глибока інспекція заголовку повідомлення (email header)
- Перевірка повідомлень за допомогою евристичних правил (heuristic)
- Виявлення спаму на основі словників заборонених слів (dictionary scan та banned word scan)
- Виявлення спаму за допомогою поведінкового аналізу (behavioral analysis)
- Виявлення спаму за допомогою перевірки IP-адреси відправника повідомлення (MTA) з IP-адресою у DNS уповноваженого MTA для певного поштового домену (Sender Policy Framework – SPF Scan)
- Виявлення спаму за допомогою перевірки підпису повідомлень приватним доменим ключом (Domain Keys Identified Mail – DKIM)
- Виявлення спаму за допомогою перевірки SPF DNS запису та DKIM підпису (Domain-Based Message Authentication - DMARC)
- Виявлення спаму під час спалахів спаму за рахунок декількох перевірок повідомлень рознесених у часі (spam outbreak)
- Виявлення підробки повідомлень, що надходять з зовнішній електронних адрес але з відображенням ім’я внутрішнього користувача (impersonation analysis / business email compromise)
- Налаштування користувацьких списків IP-адреси та адреси електронної пошти, які або звільняються від класифікації як спам, або завжди класифікуються як спам (safe list / block list)
- Налаштування користувацьких списків слів, які або звільняються від класифікації як спам (safe list word)
- Виявлення спаму завдяки аналізу графічних зображень у повідомленнях (GIF, JPG, PNG)
- Виявлення підроблення IP-адреси відправника повідомлення шляхом співставлення його IP-адреси та наявного запису канонічне ім'я хоста (forged IP)
- Виявлення спаму завдяки аналізу PDF-файлів
- Налаштування максимального розміру повідомлення для сканування (включаючи без обмежень)
- Налаштування скасування сканування повідомлень на визначення спаму для аутентифікованих сесій
- Налаштування різних дії з повідомленнями при знаходженні спами, включаючи маркування та зміну повідомлень (tag subject, insert new header)

Анти-вірус / анті-malware сервіси

- Виявлення та блокування загроз шляхом інспектування заголовків, тіла та вкладених файлів електронної пошти
- Сигнатурний антивірусний аналіз
- Евристичний антивірусний аналіз (heuristic)
- Створення власних файлів хеш-значень відомих вірусних файлів
- Імпорт та експорт файлів хеш-значень відомих вірусних файлів
- Виявлення Grayware-файлів (небажаних програми або файлів, які не класифікуються як virus/malware)
- Аналіз стислих файлів (ZIP, PKZIP, LHA, ARJ, RAR)

- Виявлення невідомих malware під час спалахів на основі репутації хеш значень файлів у базі/сервісі виробника до моменту оновлення баз на шлюзі захисту електронної пошти (virus outbreak)
- Налаштування різних дії з повідомленнями при знаходженні вірусів/malware, включаючи маркування та зміну повідомлень (tag subject, insert new header)
- Автоматичне розшифрування архівів, PDF та MS Office документів за допомогою списку паролів або виявлених слів у тілі електронної пошти
- Заміна “зараженого” файла повідомленням про заміну (replacement message), яке сповіщає користувача, що “заражений” файл був видалений
- Пересилання “зараженого” повідомлення як вкладення, залишаючи при цьому оригінальне тіло повідомлення без змін або замінюючи його (repackage email with customized or original content)

Захист від цілеспрямованих та раніше невідомих загроз

- Система має інтегруватися з системою захисту від цілеспрямованих та раніше невідомих загроз цього ТЗ, для здійснення ефективного захисту від таких загроз шляхом аналізу файлів та URI (URL) з повідомлень
- Повідомлення, що містять підозрілі вкладення не повинні перенаправлятися користувачу до закінчення інспекції (з позитивним висновком) на Sandbox

Захист на основі визначення змісту (content detection)

- Виявлення та блокування фрагментованих повідомлень
- Виявлення та блокування зашифрованих файлів, до яких не може бути підібрано пароль
- Виявлення у MIME-файлах вбудовані об’єкти та інші файли (embedded component) та сканування їх на загрози
- Визначення гранічного розміру повідомлення
- Визначення максимальної кількості вкладень у повідомлені
- Визначення типів файлів та розширення файлів, які потрібно сканувати на загрози

Захист від просунутих загроз

- Функціонал видалення або нейтралізації потенційно небезпечного вмісту (hyperlinks, macros, active scripts, javascript) у повідомленнях електронної пошти та файлах вкладень (MS Office файли, PDF-файли)
- Функціонал запобігання озброєнню раніше надійних URL-посилань після доставки повідомлення у папку "Вхідні", шляхом перевірки на загрози URL-посилання при натисканні на нього користувачем. Таки посилання мають бути перевірені на загрози системою захисту електронної пошти, при необхідності відправлені на перевірку до sandbox (time of click protection)

Керування системою

- Керування за допомогою графічного інтерфейсу (GUI) HTTPS, SSH, CLI
- Ролевий адміністративний доступ до системи на основі профілів
- Автентифікація адміністраторів – локальна база, LDAP, RADIUS, PKI
- Обмеження адміністративного доступу до системи з довірених вузлів
- Конфігурація правил, щодо стійкості паролів (Password Policy)
- Автоматичне блокування IP-адреси з якої здійснювалися спроби підбору паролю для проходження автентифікації доступу до адміністративних цілей (SSH, HTTP(S))

- Автоматичне блокування IP-адреси з якої здійснювалися спроби підбору паролю для проходження автентифікації доступу до поштових сервісів (SMTP(S), IMAP(S), POP3(S))
- REST API для конфігурації та управління системою
- Single Sign-On (SSO)
- NTP
- Формування звітів на основі журналів подій за необхідними категоріями (mail, spam, virus by sender/by recipient)
- Формування звітів за розкладом або на вимогу (on demand)
- Формування звітів у HTML та PDF-форматі та відправка їх на вказану поштову адресу
- Сповіщення за необхідними категоріями подій (системні, події безпеки) адміністраторів за допомогою
- електронною пошти
- Система має надавати детальний звіт щодо поштової статистики, виявлених загроз, поточних сесій, top-користувачів
- Моніторинг системи за допомогою SNMP v1, v2c, v3 із зовнішніх систем
- Відправка traps за допомогою SNMP v1, v2c, v3 зовнішнім системам
- Налаштування граничних параметрів для системних характеристик (CPU, memory, disk, тощо), перевищення яких буде викликати відправку SNMP traps
- Налаштування системних подій (виявлення вірусу, спаму, зміна стану інтерфейсу, тощо), виявлення яких буде викликати відправку SNMP traps
- Налаштування категорій подій (виявлення вірусу, різних системних подій, закінчення строку дійсності ліцензії, тощо), настання яких буде викликати відправку поштового повідомлення адміністраторам системи

Реєстрація подій (logging)

- Реєстрація системних подій пов'язаних з роботою безпосередньо системи
- Реєстрація подій, пов'язаних з пересилкою пошти, роботи протоколів SMTP, POP3, IMAP
- Реєстрація подій, пов'язаних з виявлення вірусів та результатами фільтрації спаму
- Забезпечення збереження журналів подій на жорсткому диску системи та на віддаленому сервері за протоколом syslog або аналогом
- Вибір рівня важливості (severity level) подій для їх реєстрації на самої системі та віддаленому сервері
- Вибір типів подій (types of log) для їх реєстрації на самої системі та віддаленому сервері
- Налаштування граничного розміру журнального файлу
- Налаштування граничного часу ведення одного журнального файлу
- Налаштування проміжку часу, через який система архівує поточний журнальний файл
- Експорт/завантаження з системи журнальних файлів у звичайному та CSV-форматі
- Кореляція усіх журнальних записів щодо певних SMTP-сесій на основі Session ID або аналогу

Звітність (reporting)

- Звіти щодо загальної поштової статистики (mail, spam, non-spam, virus, тощо)
- Звіти за відправниками різних типів повідомлень (mail, spam, virus, тощо)
- Звіти за отримувачами різних типів повідомлень (mail, spam, virus, тощо)
- Налаштування проміжку часу за який буде сформовано звіт

- Налаштування поштових доменів для який буде сформовано звіт
- Налаштування напрямку поштових повідомлень (вхідні, вихідні) для який буде сформовано звіт
- Формування звітів за розкладом (scheduled) та за потреби (on-demand)
- Звітність у форматі HTML, PDF, тощо
- Відправка звітів електронною поштою

Експертний висновок

Учасник має підтвердити наявність експертного висновку Держспецзв'язку щодо відповідності обладнання захисту електронної пошти, що він пропонує за даними торгами, вимогам нормативних документів системи технічного захисту інформації в Україні, надавши копію відповідного експертного висновку

Технічна сервісна підтримка

- Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців з рівнем сервісу 24*7
- Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7
- Постійний авторизований доступ до сайту виробника 24*7
- Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки
- Отримання основних та проміжних релізів програмного забезпечення
- Можливість реєстрації сервісних випадків в режимі 24*7

Вимоги до учасників

Вимоги до учасників

Учасники торгів повинні належним чином здійснювати діяльність щодо предмету закупівлі. У зв'язку з цим для належного захисту інтересів Замовника щодо авторизованого джерела постачання послуг за даними торгами учасники торгів **повинні надати інформаційний лист в довільний формі виданий Виробником програмного забезпечення** (від головного офісу або від регіонального офіса/штаб-квартири виробника), або його офіційним представництвом в Україні (за наявності) про партнерські взаємовідносини (з зазначенням номеру оголошення про проведення торгів з ЦБД «Прозоро» та предмету закупівлі), які гарантують (вказують на) офіційність каналу надання послуг від виробника програмного забезпечення із обов'язковим зазначенням найменування та номеру даних торгів, інформації щодо партнерських відносин між виробником програмного забезпечення та учасником процедури закупівлі.