https://prozorro.gov.ua/tender/UA-2024-11-26-019369-a

«Послуга з постачання пакетів програмного забезпечення керування вразливостями в інформаційно-телекомунікаційному середовищі» ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки

На виконання постанови КМУ від 11 жовтня 2016 р. № 710 «Про ефективне використання державних коштів» у зв'язку із необхідністю проведення закупівлі «Послуга з постачання пакетів програмного забезпечення керування вразливостями в інформаційно-телекомунікаційному середовищі» ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки для потреб Департаменту економічного розвитку Львівської міської ради - забезпечити оприлюднення обґрунтування технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення на власному веб-сайті.

1. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником:

- «Послуга з постачання пакетів програмного забезпечення керування вразливостями в інформаційно-телекомунікаційному середовищі» ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки

2. Обґрунтування технічних та якісних характеристик предмета закупівлі:

Розвиток електронного урядування, впровадження різних інструментів електронної демократії, а також технологій "розумного міста" у різних сферах життя є важливою складовою у розвитку сучасного європейського міста.

Електронне урядування забезпечує нові форми комунікації між громадянами, бізнесом та владою, безперешкодний доступ до публічної інформації сприяє участі громадян у процесах управління містом чи громадою, покращенню якості надання послуг населенню та наближенню їх до вимог мешканців.

З кожним роком формуються та, постійно оновлюючись і розширюючись, розвиваються технологічні сервіси муніципалітету, які на сьогодні охоплюють:

- офіційний сайт Львівської міської ради, електронні сервіси Гарячої лінії міста (веб-сайт та мобільний додаток) та інші веб-ресурси, впроваджені для інформування громадян про роботу виконавчих органів влади, доступу до адміністративних послуг та інших важливих муніципальних функцій, взаємодії мешканців з владою;
- сучасну систему електронного документообігу у муніципалітеті;
- електронні сервіси, які спрощують та пришвидшують систему комунікації між органами місцевої влади та мешканцями, роблять процеси відкритими та прозорими. Серед них, портал "Особистий кабінет мешканця", функціонал якого дозволяє замовляти адміністративні послуги у режимі онлайн;
- екосистема порталів та сервісів "Відкриті дані Львова", яка охоплює в себе Портал відкритих даних Львова, сайт "Панель міста", Геопортал Львова та чатбот City Helper Bot, які забезпечують доступ громадян до публічної інформації у різних зручних форматах;
- реєстр територіальної громади міста як основний ресурс, за допомогою якого реалізуються всі послуги, пов'язані з реєстрацією місця проживання населення;
- електронні сервіси для відстеження руху транспорту, які стали невід'ємними інструментами для пасажирів громадського транспорту, а також щораз популярнішим серед мешканців є електронний спосіб оплати проїзду у громадському транспорті, котрий реалізований за допомогою різних аплікацій та на завершальній стадії впровадження повноцінної автоматизованої системи оплати проїзду у громадському транспорті (електронний квиток);
- система муніципального відеоспостереження, яка щороку охоплює все більшу територію міста, використовуючи системи розпізнавання обличчя та номерних знаків автомобілів, та є невід'ємною складовою забезпечення громадського порядку у місті.

Відтак, проаналізувавши елементи електронного урядування, які впроваджені та функціонують у м. Львові, інших населених пунктах, які ввійшли до складу Львівської міської територіальної громади, а також нові виклики у сфері цифрової трансформації суспільства, пропонується нова Програма цифрового перетворення Львівської міської територіальної громади на 2021 – 2025 роки (надалі – Програма) та визначено її нові завдання.

Метою впровадження Програми є досягнення світових стандартів надання адміністративних та комунальних послуг, відкритості та доступності влади, ефективності управління господарством громади, з використанням інформаційних технологій у всіх сферах життєдіяльності.

Основними завданнями розвитку Програми є:

1. Забезпечення доступу до всіх електронних послуг та сервісів для мешканців усіх населених пунктів Львівської міської територіальної громади, зокрема через забезпечення безперешкодного доступу до високошвидкісного Інтернету у всіх населених пунктах та закладах соціальної інфраструктури на території Львівської міської територіальної громади.
2. Оновлення, консолідація та уніфікація програмних та технічних ресурсів для забезпечення гнучкості їх використання та надійної роботи інформаційно-комунікаційної інфраструктури.

3. Підтримка та вдосконалення системи інформаційної безпеки функціонування міських електронних сервісів.
4. Підвищення рівня автоматизації управлінських процесів Львівської міської ради, а також підпорядкованих комунальних підприємств та установ.
5. Впровадження електронних сервісів для оптимізації комунікації між мешканцями та виконавчою владою.
6. Впровадження проектів інформатизації для модернізації усіх сфер життєдіяльності Львівської міської територіальної громади.
7. Розвиток співпраці з ІТ-компаніями та асоціаціями ІТ-компаній.
8. Реалізація програм навчання та підвищення комп'ютерної грамотності мешканців.

Враховуючи вищенаведене викикла необхідність у проведенні закупівлі «Послуга з постачання пакетів програмного забезпечення керування вразливостями в інформаційно-телекомунікаційному середовищі» ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки із наступними технічними та якісними характеристиками:

Функціональні вимоги	
Програмний комплекс керування вразливостями в інформаційно-телекомунікаційному середовищі	
Загальні системні вимоги	Система повинна мати можливість поставки у вигляді послуги, що не потребує встановлення в ІТС або мати можливість встановлення додаткових модулів усередині ІТС для збільшення функціоналу. Система має забезпечувати можливість сканувати не менше 100 хостів у ІТС та не менше 5 FQDN.
Централізоване керування	Система повинна забезпечувати централізоване керування всім функціоналом через єдиний Веб-інтерфейс та не мати обмежень на одночасне підключення користувачів. Система повинна зберігати результати сканувань та оцінки активів у власній базі даних для можливості побудов звітів та хронології змін. База даних повинна відповідати наступним критеріям: • Не вимагати використання сторонніх баз даних для збереження результатів.
Користувачі системи	Система має підтримувати управління на основі ролей та розмежування прав доступу: • Виконання будь-якого сканування, за умови наявності політики сканування або її відсутності; • Керування користувачами; • Створення оповіщень; • Визначення та спільне використання облікових даних для сканування з наданням облікових даних; • Створення та спільне використання політик сканування; • Аудит дій користувача. Система повинна надавати можливість створення необмеженої кількості користувачів системи.
Шифрування даних, що передаються	Система має шифрувати комунікації між компонентами/модулями Системи. Система має забезпечувати шифрування комунікації між користувачами та Системою.
Продуктивність системи	Система повинна забезпечувати можливість збирання та аналізу інформації щодо наявності вразливостей з будь-яких пристроїв в ІТС, у тому числі комутаційного обладнання, маршрутизаторів, міжмережевих екранів та систем запобігання вторгненням.
Керування активами	Система повинна мати можливість без використання активного або агентського сканування, на підставі аналізу трафіку, визначати появу нових активів у мережі. При цьому система, як мінімум, повинна ідентифікувати активи за такими типами: • Сервер; • Робочі станції; • Програми; • Операційні системи; • Мережеві пристрої;

	• Віртуальні та хмарні системи; • BYOD пристрою; • Мобільні телефони; Система повинна мати можливість необмеженого інвентаризаційного сканування мережі як на розклад, так і на вимогу. Система повинна вміти пов'язувати результати сканування з активами в середовищі DHCP, де IP-адреси можуть змінюватися. Система повинна мати вбудований функціонал автоматичної класифікації та динамічного маркування певних активів у мережі, включаючи, але не обмежуючи такі критерії: • Залежно від IP підмережі; • На базі NetBIOS та FQDN імені; • на базі операційної системи. Система повинна дозволяти налаштовувати навантаження на інфраструктуру, щоб уникнути перевантаження каналів замовника під час проведення завдань сканування Система повинна автоматично запускати служби віддаленого реєстру на системах Windows під час виконання сканувань із наданням прав, а потім автоматично зупиняти ці служби після завершення сканування.
Підтримувані ОС та БД для сканування	Система повинна підтримувати, включаючи, але не обмежуючи сканування наступних операційних систем: • Microsoft Windows; • AIX; • Solaris; • HP/UX; • Linux; • Netware; • MacOS. Система повинна підтримувати, включаючи, але не обмежуючи сканування наступних баз даних: • MS SQL; • IBM DB2; • MySQL; • Oracle Database; • PostgreSQL; • Sysbase ASE; • MongoDB; • Cassandra.
Візуалізація даних (Dashboard)	Система має мати вбудований набір панелей для візуалізації даних (Dashboard). Система повинна дозволяти створювати користувацькі панелі візуалізації даних. Панелі візуалізації повинні мати автоматичне оновлення. Система має підтримувати надання спільного доступу до панелей візуалізації даних. Панелі візуалізації повинні дозволяти фільтрувати інформацію за допомогою вибору активів та ін. Система повинна дозволяти вивантажувати звіти на основі відображених панелей візуалізації даних, включаючи, але не обмежуючись форматами PDF, PNG, JPG.
Підтримка API	Система повинна надавати API для доступу до інформації, яка знаходиться в базі даних системи. Система повинна мати API для можливості інтеграції з іншими системами API має бути надана безкоштовно.
Автоматичне оновлення	Система повинна забезпечувати автоматичне оновлення конфігурацій без додаткових витрат часу з боку користувача системи.
Масштабування	Система має забезпечити просте, швидке масштабування та розширення функціоналу без необхідності додаткових інвестицій з боку купленого функціоналу.

	Система має забезпечити взаємодії географічно віддалених модулів без додаткових витрат на обслуговування. Система повинна підтримувати балансування навантаження, відновлення після збою на сканерах уразливості шляхом динамічного розподілу навантаження між сканерами на підставі наявності сканера протягом всього завдання сканування.
Сканування	Система має реалізовувати можливості: • Сканувати за розкладом; • Вмикати/вимикати необхідні тести у заданих завданнях сканування; • Зупинити завдання на потрібний час; • Мати можливість автоматично виключити критичні ресурси зі сканування, якщо вони зайняті службовими процесами згідно з розкладом; • Сканування ізольованих сегменів інфраструктури з подальшим вивантаженням результатів до центральної консолі; • Вибір уразливостей для сканування; • Сканування певних портів; • Використання облікових записів. Система повинна мати можливість при скануванні виконувати як мінімум такі типи аутентифікації: • Для OS Windows: логін і пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, Beyond Trust, Hashicorp Vault, NTLM Hash, LM Hash; • Для Unix систем: логін і пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, Beyond Trust, Hashicorp Vault, Certificate, Public Key; • Для мережного обладнання – SNMP; Система повинна мати можливість приймати цілі сканування у різних форматах: активами, IP-адресами, IP мережами, іменами. Скануючий модуль повинен встановлюватися як мінімум на наступні операційні системи: • Windows; • Linux; • MacOS; • Red Hat Enterprise Linux; • Amazon Linux 2; • Fedora. Система повинна дозволяти користувачам писати та використовувати власні перевірки під час сканування. Система повинна включати можливість додавання модуля, для пасивного сканування вразливостей, шляхом спостереження мережевого трафіку на рівні пакетів, без активного сканування систем для мереж ipv4 і ipv6. При цьому система має визначати, як мінімум: • Взаємодія між активами в інфраструктурі; • Список портів, що використовуються; • сканування портів, що виконується сторонніми системами; • Тип зашифрованих та не зашифрованих мережевих сеансів; • Передача конфіденційної інформації без використання шифрування; • уразливості у комунікаційних системах; • уразливості у протоколах, що використовуються; • вразливість у додатках. Система повинна мати можливість сканування «периметра» без необхідності розгортання додаткових модулів.
Ідентифікація вразливостей	Система повинна виявляти та класифікувати проблеми, ризики та вразливості. Також має надати докладну інформацію про характер ризику та рекомендації щодо їх мінімізації. Система повинна повідомити про відомі вразливості в активі, які повинні бути визначені консультативними організаціями в галузі безпеки (наприклад, Common Vulnerabilities and Exposures database (CVE) або The

	Open Source Vulnerability Database (OSVDB) або The SecurityFocus Bugtraq (BID) або будь-якою комбінацією з них) . База даних уразливостей продуктів повинна включати перевірки: • OS Security and Patch; • CISCO; • Firewalls; • DNS; • FTP; • SMTP; • RPC; • SNMP; • LDAP; • SMB; • CGI; • Web Servers; • Databases; • Backdoors; • Denial of Service; • Default Accounts; • Peer-To-Peer; • Remote Shell. Система повинна мати можливість: • Виявлення сервісів, які виконуються на нестандартних портах. • виявлення сервісів, не налаштованих на відображення банерів підключення. • тестувати кілька екземплярів одного й того ж сервісу, що працюють на різних портах. • сканувати «мертві вузли» (пристрої, які не відповідають команді «ping»).
Аудит	Система має надати можливість проводити аудит конфігурації та наявності виправлень у системах Windows та Unix/Linux. Система повинна надати політики аудиту для Windows, Unix/Linux, додатків, пристроїв Cisco, баз даних.
Пріоритезація	Система повинна мати можливість додаткової інтелектуальної пріоритезації, за допомогою якої система повинна визначати пріоритети вразливостей на основі ймовірності того, що кожен з них буде використаний під час атаки та поєднувати в собі незалежні джерела даних, включаючи дані про вразливості виробника та сторонні дані про вразливості та погрози. , використовуючи власний алгоритм машинного навчання виявлення вразливостей з найбільшою ймовірністю експлуатації найближчим часом.
Розвідка загроз	Система має надавати можливість переглядати інформацію про відомі вразливості, інформація про які має надходити із бази даних виробника. База даних виробника має спиратися на такі джерела, як внутрішня експертиза, рекомендації постачальників, консультативна база даних GitHub та Національна база даних вразливостей. Система має надавати категоризацію вразливостей, яка поєднує відомі показники ризику з висновками дослідницької групи виробника для виявлення найважливіших вразливостей. Функціонал категоризації вразливостей має надавати можливість розбивати ключові вразливості із бази даних виробника на категорії, включаючи, але не обмежуючись наступними категоріями: 1. Emerging Threats; 2. Recently Actively Exploited; 3. Ransomware; 4. In the news. Система має надавати можливість: 1. пошуку в базі даних вразливостей виробника; 2. профілізації вразливостей; 3. порівнювати вразливості Організації в порівнянні з відомими вразливостями.

	Пошук в базі даних вразливостей виробника має надавати можливості пошуку за CVE ID або іменем. Профіль вразливості має надавати можливість детального аналізу вразливості і включає часову шкалу подій, активи у інфраструктурі та продукти, які постраждали, джерела походження та показники, такі як профіль ризику та серйозність. Функціонал порівняння вразливостей має надавати можливість порівнювати список вразливостей із певної категорії із виявленнями в середовищі.
Виправлення вразливостей	Система має надавати функціонал створення проектів для усунення вразливостей. Система має надавати можливість відстежувати виявлення, використовуючи фільтри та групи хостів. Система має надавати можливість призначати проекти на інших користувачів. Система має надавати можливість переглядати інформацію про проект із розбивкою за тегами чи фільтрами. Система має надавати можливість аналізу тенденцій виправлення вразливостей. Система має надавати можливість динамічної зміни охоплення проекту. Система повинна надавати інформацію про вразливості і уражені активи. Система має надавати можливість створювати звіти про проекти усунення вразливостей. Система повинна надавати можливість використання готових груп фільтрів та створення власних.
Сповіщення	Система повинна підтримувати оповіщення на основі результатів сканування вразливостей чи аудиту конфігурацій. Дії повідомлень повинні включати відправку sms і e-mail повідомлень.
Звітність	Система має надавати звітність за всіма подіями, звітність має бути доступна через Веб-інтерфейс. Система повинна мати можливість генерувати звіти на запит. Система має мати вбудовані звіти. Система повинна надавати звіти щодо різних сегментів та систем у мережі. Звіти, що формуються системою, повинні як мінімум містити таку інформацію: • Назва вразливості та рівень її критичності за шкалою вендора та за CVSS; • Перелік вразливих систем чи сервісів; • Статус уразливостей; • Рекомендації щодо усунення вразливості або посилання на патч, якщо такий існує; Додаткові критерії для пріоритезації вразливості: наявність експлойта, шкідливого коду тощо.
Керування вразливостями	Система повинна відстежувати дату виявлення вразливості та дату останнього виявлення для фільтрації та формування звітів за часом знаходження вразливості в інфраструктурі. Система повинна підтримувати перевірку відсутності виправлень, наявність сервісів, перевірки відповідності аудиту файлів та інші. Система повинна надати можливість сканувати ресурси всередині, поза мережею з використанням агентів, за необхідності без агентів.
Сканування Веб-додатків	Функціонал Комплексу зі сканування (тестування) безпеки додатків (DAST) має виконувати: • Сканування Веб-додатків на наявність вразливостей з використанням авторизації або без неї; • Вказування на помилки в конфігурації; • Виконання сканування REST API на наявність вразливостей; • Проведення ssl/tls аудиту;

	Система повинна мати можливість сканування Веб-додатків на поширені вразливості, включаючи, але не обмежуючись наступним переліком: SQL injection, cross-site scripting (XSS), code injection. Для знайдених вразливостей повинна застосовуватися градація по OWASP TOP 10.
Можливості розширення	Система повинна мати можливість розширення функціоналу шляхом додавання додатків із офіційного сайту виробника. Система повинна мати можливість розширення функціоналу шляхом додавання активного та пасивного сканера. Пасивний сканер повинен забезпечувати можливість пасивного сканування вразливостей шляхом спостереження мережного трафіку без активного сканування системи.
Ліцензування	Ліцензування системи має проходити за кількістю об'єктів, що підлягають скануванню. У ліцензію мають бути включені: • Нелімітована кількість сканерів; • Нелімітована кількість агентів з повною функціональністю; • Політики аудиту системи на відповідність світовим стандартам; • Rest API.
Інтеграції	Система повинна підтримувати інтеграцію, включаючи, але не обмежуючись, з наступними рішеннями: • Amazon Web Services (AWS) – Cloud Infrastructure; • Good powered by Blackberry – MDM; • Microsoft Azure. Всі перелічені інтеграції повинні підтримуватися виробником системи.
Розгортання	Основний елемент Системи повинен постачатися як готовий до експлуатації веб-портал, розміщений поза межами IT-інфраструктури. Всі додаткові компоненти системи повинні мати можливість встановлюватися і підтримуватися як усередині, так і поза периметром IT-інфраструктури.

3. Очікувана вартість та/або розмір бюджетного призначення:

- Очікувана вартість закупівлі становить – 520 000,00 грн. з ПДВ

Відповідно до Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки, затвердженої ухвалою № 85 від 25.02.2021 «Про затвердження Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки», департамент економічного розвитку являється одним із виконавців програми (4.2.1.). На департамент покладені функції одного із реалізаторів програми, у частині забезпечення матеріально-технічної бази для впровадження електронних сервісів та засобів інформаційної безпеки для забезпечення потреб цільових груп Програми (п.4.4.1.). А також є головним розпорядником коштів Програми (6.2.). (Ухвала №85 від 25.02.2021) (https://www8.city-adm.lviv.ua/inteam/uhvaly.nsf/(SearchForWeb)/681B316687D1AE80C225868B003604D3?OpenDocument)

Рішенням виконавчого комітету № 64 від 12.01.2024 «Про затвердження на 2024 рік кошторису Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки» затверджено на 2024 рік кошторис Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки (Рішення №64) (https://www8.city-adm.lviv.ua/Pool/Info/doclmr_1.NSF/(SearchForWeb)/A7BEE902A1E0E115C2258AA2003D96AB?OpenDocument)

При визначенні очікуваної вартості замовник неухильно дотримувався принципів проведення публічних закупівель, визначених статтею 5 Закону України "Про публічні закупівлі" та враховував методи визначення очікуваної вартості предмету закупівлі, що визначені в Наказі Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі» із застосуванням методу порівняння ринкових цін. Для повноцінного аналізу ринку та належного розрахунку очікуваної вартості предмета закупівлі застосовано різнобічні джерела та ресурси отримання інформації щодо ціни, зокрема комерційні пропозиції (№4-0406-61470 від 06.11.2024, №4-0406-63796 від 18.11.2024), загальнодоступна відкрита інформація даних системи електронних закупівель Prozorro, професійного модуля аналітики bi.prozorro, електронного каталогу Prozorro.Market, а також Google пошук (огляд веб-сайтів, прайси тощо).